28 page draft "CVE Report Final Draft"

Page 01 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 25 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 26 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 27 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 28 of 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

27 page draft "CVE Current Training Assessment"

Page 01 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 25 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 26 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 27 of 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

3 page draft document "CVE Brochure"

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of ınformation and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

NATIONAL SECURITY STAFF

Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States

As a government, we are working to prevent all types of extremism that leads to violence, regardless of who inspires it. At the same time, countering al-Qa'ida's violent ideology is one part of our comprehensive strategy to defeat al-Qa'ida. Over the past 2½ years, more key al-Qa'ida leaders—including Usama bin Laden—have been eliminated in rapid succession than at any time since the September 11 attacks. We have strengthened homeland security and improved information sharing. Thanks to coordinated intelligence and law enforcement, numerous terrorist plots have been thwarted, saving many American lives.

—*President Barack Obama, August 2011*

Law enforcement and government officials for decades have understood the critical importance of building relationships, based on trust, with the communities they serve. Partnerships are vital to address a range of challenges and must have as their foundation a genuine commitment on the part of law enforcement and government to address community needs and concerns, including protecting rights and public safety. In our efforts to counter violent extremism, we will rely on existing partnerships that communities have forged with Federal, State, and local government agencies. This reliance, however, must not change the nature or purpose of existing relationships. In many instances, our partnerships and related activities were not created for national security purposes but nonetheless have an indirect impact on countering violent extremism (CVE).

At the same time, this Strategic Implementation Plan (SIP) also includes activities, some of them relatively new, that are designed specifically to counter violent extremism. Where this is the case, we have made it clear. It is important that both types of activities be supported and coordinated appropriately at the local level.

Background

The President in August 2011 signed the *National Strategy for Empowering Local Partners to Prevent Violent Extremism in the United States* (National Strategy for Empowering Local Partners), which outlines our community-based approach and the Federal Government's role in empowering local stakeholders to build resilience against violent extremism.[1] It recognizes that, as the National Security Strategy from May 2010 highlights, "our best defenses against this threat are well informed and equipped families, local communities, and institutions." To support our overarching goal of preventing violent extremists and their supporters from inspiring, radicalizing, financing, or recruiting individuals or groups in the

[1] The National Strategy for Empowering Local Partners defines violent extremists as "individuals who support or commit ideologically motivated violence to further political goals."

United States to commit acts of violence, the Federal Government is focused on three core areas of activity: (1) enhancing engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals.

The SIP details how we are implementing the National Strategy for Empowering Local Partners. It explains our core objectives and sub-objectives; describes how activities by departments and agencies are aligned with these; lists planned activities that address gaps and expand efforts; and assigns Federal Government leads and partners for various actions. The SIP provides a blueprint for how we will build community resilience against violent extremism.[2] It does not address our overseas CVE efforts, other than ensuring we coordinate domestic and international activities.

Although the SIP will be applied to prevent all forms of violent extremism, we will prioritize preventing violent extremism and terrorism that is inspired by al-Qa'ida and its affiliates and adherents, which the 2010 National Security Strategy, the 2011 National Strategy for Counterterrorism, and the National Strategy for Empowering Local Partners identify as the preeminent security threats to our country. This is, however, a matter of emphasis and prioritization, and does not entail ignoring other forms of violent extremism. As the July 2011 terrorist attack in Norway underscored, free societies face threats from a range of violent extremists.

As the activities described in the SIP are executed, there will be major and long-lasting impacts:

- There will be platforms throughout the country for including communities that may be targeted by violent extremists for recruitment and radicalization into ongoing Federal, State, and local engagement efforts;
- The Federal Government will support that engagement through a task force of senior officials from across the government;
- Community-led efforts to build resilience to violent extremism will be supported;
- Analysis will increase in depth and relevance, and will be shared with those assessed to need it, including Governor-appointed Homeland Security Advisors, Major Cities Chiefs, Mayors' Offices, and local partners;
- Training for Federal, State, tribal, and local government and law enforcement officials on community resilience, CVE, and cultural competence will improve, and that training will meet rigorous professional standards; and
- Local partners, including government officials and community leaders, will better understand the threat of violent extremism and how they can work together to prevent it.

[2] The concept of "resilience" has applied to a range of areas such as emergency preparedness and critical infrastructure protection (e.g., the ability of financial markets, power suppliers, and telecommunications companies to withstand an attack or disaster and resume operations rapidly.) The National Security Strategy emphasized the importance of including individuals and communities in our approach to enhancing resilience. Both the National Strategy for Empowering Local Partners and the 2011 National Strategy for Counterterrorism expanded this concept to CVE, the latter explicitly stating, "We are working to bring to bear many of these capabilities to build resilience within our communities here at home against al-Qa'ida inspired radicalization, recruitment, and mobilization to violence."

The SIP outlines ongoing, as well as planned, activities to counter violent extremism, which will be accomplished through existing funding and by prioritizing within the resources available to relevant departments and agencies. Some of these activities are specific to CVE, while others address broader non-security policy objectives but may have an indirect effect on countering radicalization to violence. Because our efforts are threaded across a range of different missions, such as training, outreach, and international exchanges, the execution of the SIP will be impacted by funding for both security and non-security related activities.

Process for Developing the SIP

The Obama Administration continues to prioritize and stress the critical importance of CVE in the Homeland. Given the complexities of addressing this threat and the uniqueness of the operating environment in the United States, the Administration recognizes the potential to do more harm than good if our Nation's approach and actions are not dutifully considered and deliberated. Throughout this process, careful consideration was given to the rule of law and constitutional principles, particularly those that address civil rights and civil liberties. With those principles in mind, we noted that departments and agencies with domestically focused mandates have an array of tools and capabilities that can be leveraged to prevent violent extremism, though some have limited experience in the national security arena. This necessitated a deliberative and carefully calibrated approach with an extensive evaluative period to fully address their potential roles and participation, which for some entailed thinking outside their traditional mandates and areas of work.

After assessing how individuals are radicalized and recruited to violence in the United States, the Administration established an accelerated process, led by the National Security Staff (NSS), to develop the National Strategy for Empowering Local Partners and the SIP. An Interagency Policy Committee (IPC) on countering and preventing violent extremism in the United States was established—with Assistant and Deputy Assistant Secretary-level representatives from across government—to consider roles and responsibilities, potential activities, guiding principles, and how best to coordinate and synchronize our efforts. The IPC, with support from specialist sub-IPCs, drafted our first national strategy on preventing violent extremism in the United States, which was approved by Deputies from the various departments and agencies and signed by the President.

- The following departments and agencies were involved in the deliberations and approval process: the Departments of State (State), the Treasury, Defense (DOD), Justice (DOJ), Commerce, Labor, Health and Human Services (HHS), Education (EDU), Veterans Affairs, and Homeland Security (DHS), as well as the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC).

To develop the SIP, the NSS tasked NCTC with coordinating the first comprehensive baseline of activities across the United States Government related to countering and preventing violent extremism in the United States, which constitutes the ongoing activities outlined in the SIP. This included CVE-specific initiatives, as well as activities that were not developed for CVE purposes, but nonetheless may indirectly contribute to the overall goals of the National Strategy for Empowering Local Partners. These activities were aligned with objectives and sub-objectives—based on the strategy and approved by the IPC—to

assess our overall effort and identify gaps. The IPC then considered ongoing and potential actions to address these gaps, which form the basis of planned activities outlined in the SIP. The SIP was approved by Deputies from the various departments and agencies in November 2011.

Compliance with the Rule of Law

A fundamental precept of the SIP is that the Federal Government's actions must be consistent with the Constitution and in compliance with U.S. laws and regulations. Departments and agencies are responsible for identifying and complying with legal restrictions governing their activities and respective authorities. Compliance with the rule of law, particularly ensuring protection of First Amendment rights, is central to our National Strategy for Empowering Local Partners and the execution of the SIP.

Crosscutting and Supportive Activities

There are fundamental activities that are critical to our success and cut across the objectives of the SIP. These include: (1) whole-of-government coordination; (2) leveraging existing public safety, violence prevention, and community resilience programming; (3) coordination of domestic and international CVE efforts, consistent with legal limits; and (4) addressing technology and virtual space. In many instances, these crosscutting and supportive activities describe the ongoing activities of departments and agencies in fulfilling their broader missions. As they implement new initiatives and programs in support of the SIP, departments and agencies will ensure these enabling activities appropriately guide their efforts.

1. Whole-of-Government Coordination

Leveraging the wide range of tools, capabilities, and resources of the United States Government in a coordinated manner is essential for success. Traditional national security or law enforcement agencies such as DHS, DOJ, and the FBI will execute many of the programs and activities outlined in the SIP. However, as the National Strategy for Empowering Local Partners states, we must also use a broader set of good governance programs, "including those that promote immigrant integration and civic engagement, protect civil rights, and provide social services, which may also help prevent radicalization that leads to violence." To this end, agencies such as EDU and HHS, which have substantial expertise in engaging communities and delivering services, also play a role.

This does not mean the missions and priorities of these partners will change or that their efforts will become narrowly focused on national security. Their inclusion stems from our recognition that radicalization to violence depends on a variety of factors, which in some instances may be most effectively addressed by departments and agencies that historically have not been responsible for national security or law enforcement. These non-security partners, including specific components within DOJ and DHS, have an array of tools that can contribute to this effort by providing indirect but meaningful impact on CVE, including after school programs, networks of community-based organizations that provide assistance to new immigrants, and violence prevention programs. We will coordinate activities, where appropriate, to support the CVE effort while ensuring we do not change the core missions and functions of these departments and agencies.

2. Leveraging Existing Public Safety, Violence Prevention, and Resilience Programming

While preventing violent extremism is an issue of national importance, it is one of many safety and security challenges facing our Nation. As we enter an era of increased fiscal constraints, we must ensure our approach is tailored to take advantage of current programs and leverages existing resources. Our efforts therefore will be supported, where appropriate, by emphasizing opportunities to address CVE within available resources related to public safety, violence prevention, and building resilience.

3. Coordination of Domestic and International Efforts

While always ensuring compliance with applicable laws and regulations, we must ensure a high level of coordination between our domestic and international efforts to address violent extremism. Although both the National Strategy for Empowering Local Partners and the SIP specifically address preventing violent extremism in the United States, the delineation between domestic and international is becoming increasingly less rigid. Violent extremists operating abroad have direct access to Americans via the Internet, and overseas events have fueled violent extremist radicalization and recruitment in the United States. The converse is also true: events occurring in the United States have empowered the propaganda of violent extremists operating overseas. While making certain that they stay within their respective authorities, departments and agencies must ensure coordination between our domestic and international CVE efforts. Given its mandate to support both domestic and international planning, NCTC will help facilitate this part of the CVE effort so that our Homeland and overseas activities are appropriately synchronized, consistent with all applicable laws and regulations. While individual departments and agencies will regularly engage foreign partners, all international engagement will continue to be coordinated through State.

4. Addressing Technology and Virtual Space

The Internet, social networking, and other technology tools and innovations present both challenges and opportunities. The Internet has facilitated violent extremist recruitment and radicalization and, in some instances, attack planning, requiring that we consider programs and initiatives that are mindful of the online nature of the threat. At the same time, the Federal Government can leverage and support the use of new technologies to engage communities, build and mobilize networks against violent extremism, and undercut terrorist narratives. All of our activities should consider how technology impacts radicalization to violence and the ways we can use it to expand and improve our whole-of-government effort. As noted in sub-objective 3.3, we will develop a separate strategy focused on CVE online.

Roles and Responsibilities

The SIP assigns Leads and Partners in each of the Future Activities and Efforts listed under respective sub-objectives. Leads and Partners have primary responsibility for coordinating, integrating, and synchronizing activities to achieve SIP sub-objectives and the overall goal of the National Strategy for Empowering Local Partners.

Expectation of Leads and Partners are as follows:

Lead: A department or agency responsible for convening pertinent partners to identify, address, and report on steps that are being taken, or should be taken, to ensure activities are effectively executed. The Lead is accountable for, among other things:

- Fostering communication among Partners to ensure all parties understand how to complete the activity;
- Identifying, in collaboration with assigned Partners, the actions and resources needed to effectively execute the activity;
- Identifying issues that impede progress; and
- Informing all departments and agencies about the status of progress by the Lead and other sub-objective Partners, including impediments, modifications, or alterations to the plan for implementation.

Partner: A department or agency responsible for collaborating with a Lead and other Partners to accomplish an activity. Partner(s) are accountable for:

- Accomplishing actions under their department or agency's purview in a manner that contributes to the effective execution of an activity;
- Providing status reports and assessments of progress on actions pertinent to the activity; and
- Identifying resource needs that impede progress on their department or agency's activities.

Assessing Progress

It is important to recognize that the National Strategy for Empowering Local Partners represents the first time the United States Government has outlined an approach to address ideologically inspired violent extremism in the Homeland. While the objectives and sub-objectives listed in the SIP represent the collective wisdom and insight of the United States Government about what areas of action have the greatest potential to prevent violent extremism, we will learn more about our effectiveness as we assess our efforts over time, and we will adjust our activities accordingly.

Given the short history of our coordinated, whole-of-government approach to CVE, we will first develop key benchmarks to guide our initial assessment. Where possible, we will also work to develop indicators of impact to supplement these performance measures, which will tell us whether our activities are having the intended effects with respect to an objective or sub-objective. As we implement our activities, future evaluations will shift away from benchmark performance measures towards impact assessments. Departments and agencies will be responsible for assessing their specific activities in pursuit of SIP objectives, in coordination with an Assessment Working Group. We will develop a process for identifying gaps, areas of limited progress, resource needs, and any additional factors resulting from new information on the dynamics of radicalization to violence. Our progress will be evaluated and reported annually to the President.

Objectives, Sub-Objectives, and Activities

The SIP's objectives mirror the National Strategy for Empowering Local Partners' areas of priority action: (1) enhancing Federal engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals. Each of these is supported by sub-objectives, which constitute measurable lines of effort with which our specific programs and initiatives are aligned. A key purpose of the SIP is to describe the range of actions we are taking to improve or expand these efforts.

1. Enhancing Federal Engagement with and Support to Local Communities that May be Targeted by Violent Extremists

Communication and meaningful engagement with the American public is an essential part of the Federal Government's work, and it is critical for developing local partnerships to counter violent extremism. Just as we engage and raise awareness to prevent gang violence, sexual offenses, school shootings, and other acts of violence, so too must we ensure that our communities are empowered to recognize threats of violent extremism and understand the range of government and nongovernment resources that can help keep their families, friends, and neighbors safe. As noted in the National Strategy for Empowering Local Partners:

> Engagement is essential for supporting community-based efforts to prevent violent extremism because it allows government and communities to share information, concerns, and potential solutions. Our aims in engaging with communities to discuss violent extremism are to: (1) share sound, meaningful, and timely information about the threat of violent extremism with a wide range of community groups and organizations, particularly those involved in public safety issues; (2) respond to community concerns about government policies and actions; and (3) better understand how we can effectively support community-based solutions.

At the same time, we must ensure that our efforts to prevent violent extremism do not narrow our relationships with communities to any single issue, including national security. This necessitates continuing to engage on the full range of community interests and concerns, but it also requires, where feasible, that we incorporate communities that are being targeted by violent extremists into broader forums with other communities when addressing non-CVE issues. While we will engage with some communities specifically on CVE issues because of particular needs, care should be taken to avoid giving the false impression that engagement on non-security issues is taking place exclusively because of CVE concerns. To ensure transparency, our engagement with communities that are being targeted by violent extremists will follow two tracks:

- We will specifically engage these communities on the threat of violent extremism to raise awareness, build partnerships, and promote empowerment. This requires specific conversations and activities related to security issues.
- Where we engage on other topics, we will work to include them in broader forums with other communities when appropriate.

1.1 Improve the depth, breadth, and frequency of Federal Government engagement with and among communities on the wide range of issues they care about, including concerns about civil rights, counterterrorism security measures, international events, and foreign policy issues.

Violent extremist narratives espouse a rigid division between "us" and "them" that argues for exclusion from the broader society and a hostile relationship with government and other communities. Activities that reinforce our shared sense of belonging and productive interactions between government and the people undercut this narrative and emphasize through our actions that we are all part of the social fabric of America. As President Obama emphasized, when discussing Muslim Americans in the context of al-Qa'ida's attempts to divide us, "we don't differentiate between them and us. It's just us."

Current Activities and Efforts

Departments and agencies have been conducting engagement activities based on their unique mandates. To better synchronize this work, U.S. Attorneys, who historically have engaged with communities in their districts, have begun leading Federal engagement efforts. This includes our efforts to engage with communities to (1) discuss issues such as civil rights, counterterrorism security measures, international events, foreign policy, and other community concerns; (2) raise awareness about the threat of violent extremism; and (3) facilitate partnerships to prevent radicalization to violence. The types of communities involved in engagement differ depending on the locations. United States Attorneys, in consultation with local and Federal partners, are best positioned to make local determinations about which communities they should engage. Appointed by the President and confirmed by the Senate, U.S. Attorneys are the senior law enforcement and executive branch officials in their districts, and are therefore well-placed to help shape and drive community engagement in the field.

In December 2010, 32 U.S. Attorneys' Offices began expanding their engagement with communities to raise awareness about how the United States Government can protect all Americans from discrimination, hate crimes, and other threats; to listen to concerns; and to seek input about government policies and programs. In some instances, these efforts also included initiatives to educate the public about the threat of violent extremist recruitment, which is one of many components of a broader community outreach program.

- During this initial pilot, these U.S. Attorneys significantly expanded outreach and engagement on a range of issues of interest to communities; built new relationships where needed; and communicated the United States Government's approach to CVE.
- Departments and agencies, including State, the Treasury, EDU, HHS, and DHS provided information, speakers, and other resources for U.S. Attorneys' community engagement activities, frequently partnering with DOJ on specific programs and events.

A National Task Force, led by DOJ and DHS, was established in November 2010 to help coordinate community engagement at the national level. It includes all departments and agencies involved in relevant community engagement efforts and focuses on compiling local, national, and international best practices and disseminating these out to the field, especially to U.S. Attorneys' Offices. The Task Force is also responsible for connecting field-based Federal components to the full range of United States Government officials involved in community engagement to maximize partnerships,

coordination, and resource-sharing. The following are some examples of engagement efforts that are, or will be, coordinated with the Task Force:

- The DHS Office for Civil Rights and Civil Liberties (CRCL) this year doubled its outreach to communities and expanded its quarterly engagement roundtables to 14 cities throughout the country. During Fiscal Year 2011, CRCL also conducted 72 community engagement events, some of which included CVE-related topics.
- State engaged on U.S. foreign policy with a range of interested domestic communities. The Bureau of Near Eastern Affairs alone conducted 80 outreach events over the past year.
- DOJ has produced a number of brochures and other materials on civil rights protections and steps individuals can take to prevent or respond to discrimination, and has disseminated these to various communities, including those being targeted by violent extremists. DOJ has translated these materials into a number of languages, including Arabic, Somali, Urdu, Farsi, and Hindi.
- DOJ, in coordination with DHS, expanded the Building Communities of Trust (BCOT) Initiative, which focuses on developing relationships among local law enforcement departments, fusion centers, and the communities they serve to educate communities on: (1) the Nationwide Suspicious Activity Reporting Initiative (NSI); (2) how civil rights and liberties are protected; and (3) how to report incidents in order to help keep our communities safe. DOJ continues to support the BCOT Initiative.

Future Activities and Efforts

The primary focus for the next year will be: (1) expanding the scope of engagement; (2) building new partnerships between communities and local law enforcement, local government officials, and civil society; (3) incorporating communities that are being targeted by violent extremist radicalization into broader forums with other communities to engage on a range of non-security issues; and (4) increasing our engagement specifically on CVE. Additional activities going forward include the following:

- DOJ will incorporate more U.S. Attorneys' Offices as engagement leads in the field, building on the initial U.S. Attorney-led effort. (Lead: DOJ; Partners: All)
- The National Task Force will: (1) disseminate regular reports on best practices in community engagement to local government officials, law enforcement, U.S. Attorneys' Offices, and fusion centers; (2) work with departments and agencies to increase their support to U.S. Attorney-led engagement efforts in the field; and (3) closely coordinate Federal engagement efforts with communities targeted by violent extremist radicalization. (Leads: DOJ and DHS; Partners: All)
- In consultation with Federal and local partners, the National Task Force and the U.S. Attorneys' Offices will facilitate, where appropriate, the inclusion of communities that may be targeted by violent extremist radicalization into broader engagement forums and programs that involve other communities. (Leads: DOJ and DHS; Partners: All)
- U.S. Attorneys will coordinate closely with local government officials, law enforcement, communities, and civil society to enhance outreach events and initiatives. (Lead: DOJ; Partners: All)

- In Fiscal Year (FY) 2012, CRCL plans on expanding its quarterly community engagement roundtables to a total of 16. CRCL is also in the process of implementing a campus youth community engagement plan, through which it will engage with young adults on the topic of violent extremism. (Lead: DHS)
- Depending on local circumstances, and in consultation with the FBI and other agencies as appropriate, U.S. Attorneys will coordinate any expanded engagement specific to CVE with communities that may be targeted by violent extremist radicalization. (Lead: DOJ; Partners: DHS, NCTC, and FBI)
- An FBI CVE Coordination Office will be established and, as part of its activities, will coordinate with the National Task Force on CVE-specific education and awareness modules. These modules will be developed and implemented, in part, by leveraging some of the FBI's existing programs and initiatives. (Lead: FBI; Partners: DOJ and DHS)
- DHS will oversee an online portal to support engagement by government officials and law enforcement with communities targeted by violent extremist radicalization, which will be used to share relevant information and build a community of interest. The portal will be accessible to government officials and law enforcement involved in overseas and domestic CVE and community engagement efforts to share best practices. (Lead: DHS; Partners: State, and NCTC)
- DOJ will expand the efforts of the BCOT initiative to help facilitate trust between law enforcement and community leaders. This dialogue could include local issues, as well as CVE. (Lead: DOJ; Partner: DHS)
- The United States Government will build a digital engagement capacity in order to expand, deepen, and intensify our engagement efforts. Where possible, virtual engagement will build on real world engagement activities and programs. (Lead: DHS; Partners: All)

1.2 *Foster community-led partnerships and preventative programming to build resilience against violent extremist radicalization by expanding community based solutions; leveraging existing models of community problem-solving and public safety; enhancing Federal Government collaboration with local governments and law enforcement to improve community engagement and build stronger partnerships; and providing communities with information and training, access to resources and grants, and connections with the philanthropic and private sectors.*

The Federal Government can foster nuanced and locally rooted counter-radicalization programs and initiatives by serving as a facilitator, convener, and source of information to support local networks and partnerships at the grassroots level. Importantly, because the dynamics of radicalization to violence frequently vary from location to location, we recognize that a one-size-fits-all approach will be ineffective.

Current Activities and Efforts

The Federal Government has held a series of consultative meetings with communities, local government and law enforcement, civil society organizations, foundations, and the private sector to better understand how it can facilitate partnerships and collaboration. This leverages a key strength identified

in the National Strategy for Empowering Local Partners: "The Federal Government, with its connections to diverse networks across the country, has a unique ability to draw together the constellation of previously unconnected efforts and programs to form a more cohesive enterprise against violent extremism." Examples of this include the following:

- DHS Secretary Napolitano tasked her Homeland Security Advisory Council (HSAC) to develop recommendations on how the Department can best support law enforcement and communities in their efforts to counter violent extremism. An HSAC CVE Working Group convened multiple meetings with local law enforcement, local elected officials, community leaders (including faith-based leaders), and academics. The working group released its recommendations in August 2010, highlighting the importance of: (1) research and analysis of violent extremism; (2) engagement with communities and leveraging existing partnerships to develop information-driven, community-based solutions to violent extremism and violent crime; and (3) community oriented policing practices that focus on building partnerships between law enforcement and communities.
- DHS and NCTC began raising awareness about violent extremism among private sector actors and foundations and connected them with community civic activists interested in developing programs to counter violent extremism. DHS is now working with a foundation to pilot resiliency workshops across the country that address all hazards, including violent extremism.

We also began exploring how to incorporate CVE as an element of programs that address broader public safety, violence prevention, and resilience issues. This has the advantage of leveraging preexisting initiatives and incorporates CVE in frameworks (such as safeguarding children) used by potential local partners who may otherwise not know how they fit into such efforts. For example, although many teachers, healthcare workers, and social service providers may not view themselves as potentially contributing to CVE efforts, they do recognize their responsibilities in preventing violence in general. CVE can be understood as a small component of this broader violence prevention effort. Departments and agencies will review existing public safety, violence prevention, and resilience programs to identify ones that can be expanded to include CVE as one among a number of potential lines of effort.

- As an example, the Federal Government helped support a community-led initiative to incorporate CVE into a broader program about Internet safety. The program addressed protecting children from online exploitation, building community resilience, and protecting youth from Internet radicalization to violence.

Future Activities and Efforts

Planned activities to expand support to local partners include the following:

- The Federal Government will help broker agreements on partnerships to counter violent extremism between communities and local government and law enforcement to help institutionalize this locally focused approach. (Lead: DHS)
- DHS and DOJ will work to increase support for local, community-led programs and initiatives to counter violent extremism, predominantly by identifying opportunities within existing appropriations for incorporating CVE as an eligible area of work for public safety, violence prevention, and community resilience grants. (Leads: DHS and DOJ)

- DHS is working to increase funding available to integrate CVE into existing community-oriented policing efforts through FY12 grants. (Lead: DHS)
- DHS is establishing an HSAC Faith-Based Community Information Sharing Working Group to determine how the Department can: (1) better share information with faith communities; and (2) support the development of faith-based community information sharing networks. (Lead: DHS)
- DHS is developing its Hometown Security webpage to include resources such as training guidance, workshop reports, and information on CVE for both the general public and law enforcement. (Lead: DHS)
- The Treasury will expand its community outreach regarding terrorism financing issues. (Lead: Treasury; Partners: State, DOJ, DHS, FBI, and the U.S. Agency for International Development)[3]
- Depending on local circumstances and in consultation with the FBI, U.S. Attorneys will coordinate, as appropriate, any efforts to expand connections and partnerships at the local level for CVE, supported by the National Task Force where needed. (Lead: DOJ; Partners: All)
- Departments and agencies will expand engagement with the business community by educating companies about the threat of violent extremism and by connecting them to community civic activists focused on developing CVE programs and initiatives. (Lead: DHS; Partner: NCTC)

2. Building Government and Law Enforcement Expertise for Preventing Violent Extremism

It is critical that the Federal Government and its local government and law enforcement partners understand what the threat of violent extremism is, and what it is not. This helps ensure that we focus our resources where they are most effective and that we understand how we can best empower and partner with communities. Building expertise necessitates continued research about the dynamics of radicalization to violence and what has worked to prevent violent extremism; sharing this information as widely as possible; and then leveraging it to train government officials and law enforcement.

2.1 Improve our understanding of violent extremism through increased research, analysis, and partnerships with foreign governments, academia, and nongovernmental organizations.

The Federal Government has built a robust analytic program to understand violent extremism that includes analysis; research conducted by academia, think tanks, and industry; and exchanges with international allies to identify best practices. While we have increased our understanding of how individuals are radicalized to violence, we must continue to identify gaps, monitor changes in the dynamics of violent extremism, and remain vigilant by challenging our assumptions and continuing our research and analysis.

Current Activities and Efforts

The United States Government's research capacity on this issue has greatly expanded. DHS and NCTC both have analytic groups exclusively focused on violent extremist radicalization; the Interagency Intelligence Subcommittee on Radicalization helps coordinate and improve CVE intelligence analysis; and we work with foreign governments, academia, and nongovernmental organizations to inform and

[3] The U.S. Agency for International Development's role will be limited to sharing relevant information.

supplement our analysis and understanding. In addition to a large volume of intelligence products on CVE, examples of activities include:

- DHS Science & Technology (S&T) sponsored research on violent extremism in the United States, which it has shared with DHS components and other departments and agencies. Over 20 reports have been produced since 2009 and 5 more will be produced by the end of 2011. DHS is also developing an integrated open source database to help inform CVE programs.
- DHS's Office of Intelligence and Analysis (I&A) collaborated with the FBI, the Bureau of Prisons (BOP), and NCTC to assess the capacity of state correctional institutions to detect and share information regarding individuals who demonstrate behaviors associated with violent extremism while in the correctional system.
- The National Intelligence Council, DHS, FBI, and NCTC briefed fusion centers and law enforcement around the country on violent extremism.
- DHS, in partnership with the FBI and NCTC, developed case studies on preoperational indicators and known threats for State and local law enforcement and affected communities.
- The United States Government held regular exchanges of best practices with Australia, Canada, Denmark, Germany, the European Union, the Netherlands, the United Kingdom, and other partners to gain comparative insights about what might be effective in the Homeland.
- DHS expanded cooperation between the United States and Canada on CVE research and lessons learned.
- The United States Government participates in the Global Counterterrorism Forum's CVE Working Group.
- As directed in the Fort Hood Follow-on Review, DOD established the Force Protection Senior Steering Group. Among the Steering Group's duties is the coordination of non-traditional partners' activities within DOD (e.g., counterintelligence and behavioral health) to better understand how to identify and prevent all forms of violent extremism—not limited to al-Qa'ida-inspired extremism—within the military, including the potential use of DOD's extensive network of programs designed to support individuals who are potentially at risk of committing acts of violence against themselves, their families, or co-workers.

Future Activities and Efforts

Although we have a better understanding of the threat, there are gaps that need to be addressed through additional research and analysis. In this regard, we will:

- Expand analysis in five priority areas (Leads: DHS, FBI, NCTC, and State):
  1. The role of the Internet in radicalization to violence and how virtual space can be leveraged to counter violent extremism.
  2. Single-actor terrorism (so called "lone wolves"), including lessons learned from similar phenomena such as a school shooters.
  3. Disengagement from terrorism and violent extremism.

4. Non-al-Qa'ida related radicalization to violence and anticipated future violent extremist threats.
5. Preoperational indicators and analysis of known case studies of extremist violence in the United States.

- Continue DHS S&T's support for research on countering the threat of extremist violence. (Lead: DHS)
- Continue DHS collaboration with the FBI, the BOP, and NCTC to: (1) improve awareness of the risk of violent extremism in correctional systems; (2) enhance screening of new inmates to detect individuals associated with violent extremist organizations; (3) improve detection of recruitment efforts within the correctional environment; and (4) increase information sharing, as appropriate, with Federal, State, and local law enforcement about inmates who may have adopted violent extremist beliefs and are being released. (Lead: DHS; Partners: DOJ, FBI, and NCTC)
- Complete the creation of the FBI CVE Coordination Office to help assess and leverage existing Bureau efforts to better understand and counter violent extremism. (Lead: FBI)
- Build lines of research specifically to support non-security Federal partners. (Leads: DHS and NCTC; Partners: EDU and HHS)

2.2 Increase Federal Government information sharing with State, local, and tribal governments and law enforcement on terrorist recruitment and radicalization.

As we enhance our partnerships with State, local, and tribal governments and law enforcement to counter violent extremism, it is essential that we share our expertise and insights about the dynamics of radicalization to violence and what has worked to prevent it. This, in turn, will help our partners identify potential areas of collaboration with communities and other local actors.

Current Activities and Efforts

Examples include:

- Based on direction from the Office of the Director of National Intelligence (DNI), DHS led an effort to improve the analysis of homegrown violent extremism, including analytic tools to share with State, local, and tribal partners. DHS briefed representatives of 47 states on the project.
- DHS generated case studies of known and suspected terrorists and assessments of radicalization to violence, based on recent arrests, to share with local partners.
- FBI disseminated information to public safety partners, including information about radicalization to violence.
- DHS, NCTC, and FBI briefed and disseminated information on how individuals are radicalized to violence to law enforcement, fusion centers, and local government officials, including the Major Cities Chiefs, representatives from 47 states, Mayors' Offices, and State Homeland Security Advisors.

- In partnership with NCTC, DOJ, DNI, and FBI, DHS led the first National CVE Workshop in August 2011, which brought together intelligence commanders from major metropolitan areas and fusion center directors to increase their understanding of CVE.

Future Activities and Efforts

More work needs to be done to ensure our State, local, and tribal partners have the information they need to counter violent extremism. Classification remains an obstacle to broader sharing with these partners, but we can better ensure that analytic production is tailored to the needs of practitioners in the field. Major work over the next year will focus on creating more analytic products on CVE that directly support local law enforcement and government. Planned actions include:

- Development of an analytic team focused on supporting local government and law enforcement CVE practitioners and increased production of analysis at appropriate classification levels. (Lead: DHS; Partners: FBI and NCTC)
- Development of practitioner-friendly summaries of current research and literature reviews about the motivations and behaviors associated with single-actor terrorism and disengagement from violent extremism. (Lead: DHS)
- Review of information-sharing protocols to identify ways of increasing dissemination of products to State, local, and tribal authorities. (Leads: DHS, DOJ, FBI, and NCTC)
- Expansion of briefings and information sharing about violent extremism with State and local law enforcement and government. (Lead: DHS, FBI, and NCTC)

2.3 *Improve the development and use of standardized training with rigorous curricula based on the latest research, which conveys information about violent extremism; improves cultural competency; and imparts best practices and lessons learned for effective community engagement and partnerships.*

The Federal Government has expanded and improved training related to CVE over the past year, but challenges remain. In particular, there is a need for a review process and standards for training specific to CVE, which was underscored by a small number of instances of Federally sponsored or funded CVE-related and counterterrorism training that used offensive and inaccurate information, which was inconsistent with our values and core principles. As our National Strategy to Empower Local Partners highlights, "Misinformation about the threat and dynamics of radicalization to violence can harm our security by sending local stakeholders in the wrong direction and unnecessarily creating tensions with potential community partners." Therefore, improving Federal Government-approved training practices and processes related to CVE is a top priority of this plan.

Current Activities and Efforts

In November 2010, the IPC tasked DHS to form an Interagency Working Group on Training to catalogue and recommend improvements for CVE-related training across government. The Working Group brought together individuals responsible for CVE training and substantive specialists from civil rights and civil liberties offices, Federal law enforcement, and the analytic community. This is part of our overall

emphasis on improving the quality and quantity of CVE-related training. Notable accomplishments in our efforts to improve training include:

- Between October 2010 and October 2011, DHS CRCL trained nearly 2,700 law enforcement officials on CVE and cultural awareness at 46 separate events. The training served as the basis for best practices recommended by the Interagency Working Group on Training.
- Based on input from participating agencies, DHS issued CVE training guidance and best practices in October 2011 for Federal, State, local, and tribal government officials charged with organizing training related to CVE, cultural awareness, and counterterrorism.
- The Federal Emergency Management Agency (FEMA) in October 2011 issued an Information Bulletin on CVE Training, which includes DHS's training guidance and best practices, as well as guidance for State, local, and tribal entities that regularly leverage FEMA grants to fund CVE-related trainings. DHS sent the best practices paper and the FEMA guidance to all DHS grantees, State and local governments, State and local law enforcement, relevant community stakeholders, and interagency partners.
- DHS provided a full-day of training, which included training on cultural competency, civil rights, and civil liberties to Federal, State, local, and tribal partners at 12 fusion centers in the past year and over 30 fusion centers since 2008. These trainings were coupled with 3- to 4-hour CVE training sessions for State and local law enforcement operating in the same state. Additionally, DHS provided "train the trainer" sessions for staff from nearly all fusion centers nationwide.
- DHS, working closely with other departments and agencies, local law enforcement, academics, and curriculum development experts, developed guidelines for a CVE curriculum that focuses on information-driven community-oriented policing practices and how to leverage existing community partnerships to counter violent extremism and violent crime. These guidelines were reviewed and validated in February 2011 at a "proof-of-concept" session at the Federal Law Enforcement Training Center (FLETC), which was attended by State, local, and tribal law enforcement executives and frontline officers from rural and major city jurisdictions.
- State, working closely with NCTC and DHS, piloted specialized CVE training for United States Government officials working on CVE in the United States and abroad through its Foreign Service Institute in May 2011. Participation by domestic and international practitioners provided opportunities for exchanging best practices, enhanced the coordination of our Homeland and overseas efforts, and encouraged interagency partnerships.

Future Activities and Efforts

A review process by the Interagency Working Group on Training, as well as internal assessments by departments and agencies, indentified two key challenges, which we will address over the next year:

- Many departments and agencies lack a review process for training materials and outside speakers on CVE, which led to a small number of cases of training that violated internal principles as well as core tenets of the National Strategy to Empower Local Partners.

- There has been a lack of guidance and standards for training related to CVE, which left field offices, in particular, vulnerable to bad training. Without guidance or standards, it has been difficult to enforce accountability.

We have prioritized addressing these two shortcomings by doing the following:

- Departments and agencies are taking steps to identify training materials that may not meet internal standards and to improve processes for creating and reviewing such materials. Some departments are consulting with outside experts with established reputations to evaluate the content and training review process. Guidance on CVE-related training is being developed and will be issued, both across the organizations and to field components. Some departments may issue this as part of broader training guidance. (Lead: All)
- DHS, via FLETC, is in the process of developing a CVE curriculum to be integrated into existing training programs for Federal law enforcement. The curriculum will give Federal law enforcement a better understanding of CVE and how to more effectively leverage existing local partnerships. (Lead: DHS)
- DHS is in the process of establishing an internal committee to review all directly funded and issued DHS training on cultural competency, engagement, CVE, and counterterrorism. The committee will be responsible for reviewing any new content, evaluating experts, and establishing quality control. FEMA will incorporate the recently released Informational Bulletin and training guidance into FY12 grant guidance and will also leverage existing mechanisms to hold grantees and sub-grantees accountable. (Lead: DHS)

In addition to addressing the quality issue, we will work to expand the quantity of training.

- DHS, in partnership with the Los Angeles Police Department and the National Consortium for Advanced Policing, is developing a CVE curriculum that includes a 16-hour continuing education module for executive and frontline officers, as well as a 30-minute module that will be introduced at police academies. Both will be certified by the Police Officers Standards and Training Council. In October 2011 the Major Cities Chiefs Association passed a motion to adopt and implement the DHS CVE curriculum, which will be piloted with State and local law enforcement in San Diego by the end of 2011. By 2013, DHS seeks to: (1) implement the curriculum across the country on a regional basis; (2) develop a national network of trainers and subject matter experts who can administer the training and keep it current; and (3) build an online component for the curriculum. (Lead: DHS; Partners: DOJ and NCTC)
- DHS, via FLETC, will update current Federal training programs to integrate the CVE curriculum for Federal law enforcement in the coming year. (Lead: DHS)
- DHS is working with European law enforcement partners to share best practices and case studies to improve training, community policing, and operational information sharing. (Lead: DHS)
- DHS CRCL is expanding and institutionalizing its CVE and cultural competence training curricula to further enhance the material and its effectiveness. (Lead: DHS)

- The Interagency Working Group on Training will facilitate a "train the trainer program" to increase the reach of CVE training. (Leads: DHS and NCTC; Partners: DOJ, EDU, HHS, and FBI)
- The Interagency Working Group on Training will facilitate the development of an online training program that provides professional development credit for a broad range of professions, particularly those involved with public safety, violence prevention, and resilience. This will help build a basic understanding of CVE among a broad cross-section of stakeholders who have related mandates. (Leads: DHS and NCTC; Partners: DOJ, FBI, EDU, and HHS)
- The Interagency Working Group on Training will collaborate with non-security partners, such as EDU, to build CVE training modules that can be incorporated, as appropriate, into existing programs related to public safety, violence prevention, and resilience. These modules will be crafted in a way that is relevant to the specific audiences and their missions. Only trainers who have undergone CVE-specific training will deliver training programs that include CVE modules. (Lead: DHS; Partners: DOJ, EDU, HHS, FBI, and NCTC)
- DOD's training programs and curricula will be informed by the work of the Interagency Working Group on Training, as appropriate. Additionally, DOD is conducting a review of CVE-related curricula and will make revisions and adjustments as necessary. (Lead: DOD; Partner DHS)

3. Countering violent extremist propaganda while promoting our ideals

As the National Counterterrorism Strategy emphasizes, "[t]he United States was founded upon a belief in a core set of values that is written into our founding documents and woven into the very fabric of our society. Where terrorists offer injustice, disorder, and destruction the United States must stand for freedom, fairness, equality, dignity, hope, and opportunity. The power and appeal of our values enables the United States to build a broad coalition to act collectively against the common threat posed by terrorists, further delegitimizing, isolating, and weakening our adversaries."

Countering the ideologies and narratives that legitimize violence is central to our effort, but it also is the most challenging area of work, requiring careful consideration of a number of legal issues, especially those related to the First Amendment. In many instances, it will be more effective to empower communities to develop credible alternatives that challenge violent extremist narratives rather than having the Federal Government attempt to do so.

Our efforts include not only challenging justifications for violence, but affirming American ideals of inclusiveness and opportunity as well. Violent extremist narratives feed on disenchantment and the sense of exclusion. Our efforts therefore must include positive affirmation of our unity as a country. To some extent, this is addressed through our engagement activities, particularly where they address challenges facing all communities and not just those targeted by violent extremist radicalization. But there are also situations where we will need to more directly challenge violent extremist narratives.

3.1 Increase the capacity of communities to directly challenge violent extremist ideologies and narratives.

While the government cannot always directly contest violent extremist ideas, it can support capacity building within communities to take on this role. Whereas sub-objective 1.2 emphasizes preventative

measures and a defensive posture to build capacity for enhancing community resilience, sub-objective 3.1 focuses on increasing the ability of communities to push back against violent extremist propaganda.

Current Activities and Efforts

Most of our work in this area to date has focused on connecting community activists to potential civil society and private sector partners to focus specifically on undermining violent extremist narratives. Over the past year, we have taken the following steps:

- NCTC in 2010 developed a Community Awareness Briefing (CAB) to inform members of the public about efforts by al-Qa'ida and its adherents and affiliates to recruit Americans. The CAB highlights recruiting videos and examples of violent extremist propaganda, while underscoring the fact that these materials are often easily available on the Internet. Most importantly, the CAB aims to facilitate a discussion about what government and communities can do, together and independently, to counter the threat of violent extremist narratives. NCTC continues to deliver the presentation at forums composed of community leaders, educators, and parents in cities across the United States. In March 2011, NCTC held a workshop for local, State, and field-based Federal officials on how the CAB could be used in engagement efforts, when it makes sense and is appropriate.
- NCTC connected civic activists with technology experts, resulting in a training seminar on how to maximize the use of technology to counter violent extremism online.
- State sponsored speaker series and exchanges between international CVE practitioners and American communities targeted by violent extremist recruiters to better understand effective models for countering violent extremist narratives.

Future Activities and Efforts

This is a nascent area of effort and therefore will necessitate greater focus over the next year. Our planned actions include:

- Expanding efforts to raise community awareness about the threat of radicalization to violence, building from the experience of the CAB, and adapting those materials for different audiences where appropriate. (Leads: DOJ, DHS, FBI, and NCTC)
- Learning from former violent extremists, specifically those who can speak credibly to counter violent narratives, provide insights to government, and potentially catalyze activities to directly challenge violent extremist narratives. (Lead: DHS; Partner: NCTC)
- Providing grants to counter violent extremist narratives and ideologies, within authorities and relevant legal parameters, by reprioritizing or increasing the flexibility of existing funding. (Lead: DHS)
- Brokering connections between private sector actors, civil society, and communities interested in countering violent extremist narratives. (Lead: DHS; Partner: NCTC)
- Promoting international exchange programs to build expertise for countering violent extremist narratives. (Lead: State; Partners: DDJ, DHS, FBI, and NCTC)

- Increasing technical training to empower communities to counter violent extremists online, including the development of training for bloggers. (Lead: DHS; Partners: State, NCTC, and FBI)

3.2 *Improve and increase our communication to the American public about the threat posed by violent extremist groups, myths and misperceptions about violent extremist radicalization, and what we are doing to counter the threat.*

It is important that we communicate to the American public the realities of what the threat is, and what it is not. Misconceptions about the threat and statements and actions that cast suspicion on entire communities based on the actions of a few distract attention from the real threat and can undermine our ability to build partnerships. An informed citizenry enhances our national security.

Current Activities and Efforts

In 2011, the Federal Government focused on developing its approach to domestic CVE and communicating this to the American public. This involved briefings to Congress, public addresses, and media interviews. We will continue these activities.

Future Activities and Efforts

In 2012, we will work to expand our efforts to raise awareness in the general public about radicalization to violence in the United States and the tools to prevent it by:

- Providing regular briefings to Congress, think tanks, and members of the media. (Lead: DHS; Partners: DOJ, FBI, and NCTC)
- Creating programs to directly engage the public on the issue. (Lead: All)
- Building a public website on community resilience and CVE. (Lead: DHS)

3.3 *Build a strategy to leverage new technologies and address online violent extremist radicalization*

The Internet has become an increasingly potent element in radicalization to violence, enabling violent extremists abroad to directly communicate to target audiences in the United States. This direct communication allows violent extremists to bypass parents and community leaders. The SIP specifically addresses the online arena in several sub-objectives, but because of the importance of the digital environment, we will develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience that considers: (1) the latest assessment of the role of the Internet; (2) the absence of clear national boundaries in online space and the relationship between international and domestic radicalization to violence; (3) relevant legal issues; and (4) the differing authorities and capabilities of departments and agencies.

Conclusion

Protecting our Nation's communities from violent extremist recruitment and radicalization is a top national security priority. It is an effort that requires creativity, diligence, and commitment to our fundamental rights and principles. In his cover letter to the National Strategy for Empowering Local Partners, President Obama wrote:

> Sadly, the threat of violent extremism in America is nothing new. Throughout our history, misguided groups—including international and domestic terrorist organizations, neo-Nazis and anti-Semitic hate groups—have engaged in horrific violence to kill our citizens and threaten our way of life. Most recently, al-Qa'ida and its affiliates have attempted to recruit and radicalize people to terrorism here in the United States, as we have seen in several plots and attacks, including the deadly attack 2 years ago on our service members at Fort Hood. As a government, we are working to prevent all types of extremism that leads to violence, regardless of who inspires it.
>
> —President Barack Obama, August 3, 2011

A complex issue like violent extremist radicalization and recruitment requires a nuanced path to guide a whole-of-government approach. The SIP outlines this path and facilitates a division of labor by assigning responsibilities between Federal Government departments, agencies, and components focused on law enforcement and national security and those whose efforts support, but do not directly lie within, these areas.

3 page draft document "The role of fusion centers in countering violent extremism"

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: Henkels, Suzanne (b)(6)
(b)(6)

To: "Simmons, Caroline (b)(6)
(b)(6)
"Barry, Patrick </O=
(b)(6)

CC: "Duggan, Alaina <(b)(6)
(b)(6)
"Snyder, Nathanie
(b)(6)
"Lee, SY </O=DH
"Houser, Jason <
(b)(6)

Subject: RE: Interview with New York Times

Date: 2012/03/29 17:09:54

Priority: Normal

Type: Note

This is awesome! Thank you all for your hard work on this – I know it was quite a lift!

From: Simmons, Caroline
Sent: Thursday, March 29, 2012 5:08 PM
TD: Barry, Patrick; Henkels, Suzanne
Cc: Duggan, Alaina; Snyder, Nathaniel; Lee, SY; Houser, Jason
Subject: RE: Interview with New York Times

Hi Suzanne,
Below are more detailed talking points from our team. Let us know if you need any additional information. Thanks for your patience with this!
Best regards,
Caroline

1. **Organization and Planning to Improve Counterterrorism Coordination**

- Following the attempted attack on December 25, 2009, I directed Rand Beers to be the Department's Coordinator for Counterterrorism in order to better coordinate counterterrorism activities across the Department's directorates, components, and offices related to detection, prevention, response to, and recovery from acts of terrorism.
- This includes syncing intelligence with operators in relevant components; breaking down obstacles that prevent components from responding to threats with appropriate countermeasures; and identifying systemic challenges afflicting the department.

- The CT Coordinator also chairs the Counterterrorism Advisory Board (CTAB), which serves as a consistent, high-level forum for coordination on counterterrorism among DHS components.

- The CTAB brings together the intelligence, operational and policy-making elements within DHS headquarters and its components.

- The CTAB has been an integral coordinating body that has assisted in responding to numerous threat streams in the past year. For example, the CTAB was the main body coordinating all of the Department's countermeasures in the lead up to the 10th Anniversary of 9/11. The CTAB also successfully coordinated the Department's countermeasures during the 2011 Holiday period and it continues to engage in intelligence review and operational coordination regarding potential threat streams.

Enhanced Domestic Capabilities to Detect and Prevent Terrorist Attacks

➢ **Information Sharing**

- DHS has more efficiently and effectively disseminated information to State and Local Law Enforcement, through Joint Intelligence Bulletins (JIBS), Intelligence Briefings, and Outreach to Federal, State, Local, Private Sector, and other community partners on the new National Terrorism Alert System (NTAS).

➢ **Support for State and Local Law Enforcement**

- DHS has helped establish a more robust grassroots analytic capability at fusion centers by ensuring that national intelligence is analyzed and applied to a local context to enable better operational planning for state and local law enforcement. DHS has also enhanced law enforcement and intelligence community information to support investigations, and locally-focused analytical work.

➢ **Standardizing Training for Officers to Report Suspicious Activities**

- In March 2010, the Nationwide SAR Initiative (NSI) Program Management Office (PMO) was established within the U.S. Department of Justice (DOJ), Bureau of Justice Assistance, and is an interagency office composed of representatives from DOJ, DHS, FBI, and the PM-ISE.
- DHS and DOJ have trained over 190,000 frontline officers through the SAR Initiative and hope to reach all of America's officers on the frontlines.

➢ **Raising Community Awareness**

- DHS has established the "If You See Something, Say Something (TM)", a simple and effective program to raise public awareness of indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the authorities.
- Some of the most recent partnerships include the Super Bowl in Indianapolis, this was the second year in a row the Department partnered at the Super Bowl and for the security awareness brief provided a few days before the Super Bowl the Secretary traveled to Indianapolis to take part in it.
- In Florida we have partnered with the State along with many private sector partners to include the NBA at this year's All-Star Jam Session and with the Miami Heat and Orlando Magic, also, a few weeks ago we partnered with the Brickyard 400 in St. Petersburg.

Efforts to Counter Violent Extremism (CVE)

➢ **Overall CVE Approach**

- The White House CVE strategy was released in August, 2011. On December 8, 2011, the White House released the Strategic Implementation Plan (SIP) for the Administration's CVE Strategy. The SIP lists the current and future actions the USG will take in support of a locally-focused, community-based approach, in three broad areas: 1) Enhancing engagement and support to local communities; 2) Building government and law enforcement expertise; and 3) countering violent extremist propaganda. The SIP directly supports the DHS CVE Approach which was informed based on the recommendations from the HSAC CVE Working Group that were issued in August, 2010,

- DHS worked closely with the White House, NCTC, DOJ, and the FBI to develop the SIP, and will continue to work closely with these entities in implementing the priorities in the SIP. In support of the SIP, DHS is working on the following key initiatives:

➢ **CVE Training**

- **Overall Training** - DHS is working with state, local, tribal and federal partners to develop a CVE Curriculum for state, local, tribal, and federal law enforcement as well for use at academies.
- **DHS CVE Training for State and Local Law Enforcement** – DHS, in conjunction with the LAPD and the National Consortium for Advanced Policing (NCAP) held the CVE Curriculum Pilot for State, Local and Tribal Law Enforcement in San Diego, CA on January 25-27, 2012 for officers from San Diego PD, LAPD, LASD, San Diego Harbor PD, and other area law enforcement agencies (approximately 45 students). The curriculum will undergo further review and editing and further pilots will be conducted. The Major Cities Chiefs Association also passed a motion to adopt and implement the DHS CVE curriculum in their training academies.
- **DHS CVE Training for Federal Law Enforcement** – On February 16, 2012, DHS/FLETC hosted a full day conference on CVE for their training staff in order to better understand the administration and DHS' CVE approach. DHS/I&A, S&T, CRCL, and NCTC provided presentations on the behaviors and indicators of violent extremism, and FLETC is working to incorporate their findings into their federal training curriculum.
- **DHS CRCL Training** - To date, CRCL has already trained more than 2,100 police officers on ways to counter violent extremism in their own communities.
- **DHS Training for Correctional Facility Officers** - DHS, in conjunction with the Interagency Threat Assessment and Coordination Group (ITACG) piloted a CVE training for Correctional Facility Officers on March 28, 2012 in Maryland.

➢ **International Partnerships**

- **DHS Work with Europol** – DHS is working closely with Europol to share information best practices at fusion centers; CVE training; increased information sharing between US fusion centers and EU fusion centers; and, improved knowledge of behaviors and indicators of violent extremism among DHS and European law enforcement. DHS along with DOJ, NCTC, the FBI, and 5 State and Local Law Enforcement Representatives attended a Europol-U.S. CVE Conference at Europol Headquarters on March 19-21, 2012 to exchange case studies and behaviors and indicators on violent extremism, and CVE training curricula.

From: Barry, Patrick
Sent: Thursday, March 29, 2012 4:38 PM
To: Henkels, Suzanne
Cc: Duggan, Alaina; Simmons, Caroline; Snyder, Nathaniel; Lee, SY; Houser, Jason
Subject: RE: Interview with New York Times

Hey, we should be wrapping this up soon. Caroline is packaging it, and I think we're still waiting on some input from Jason.

From: Henkels, Suzanne
Sent: Thursday, March 29, 2012 4:26 PM

To: Barry, Patrick
Cc: Duggan, Alaina; Simmons, Caroline; Snyder, Nathaniel; Lee, SY; Houser, Jason
Subject: RE: Interview with New York Times

Just wanted to check in to see if there was anything that we could do to help. Thanks!

From: Barry, Patrick
Sent: Thursday, March 29, 2012 9:04 AM
To: Henkels, Suzanne
Cc: Duggan, Alaina; Simmons, Caroline; Snyder, Nathaniel; Lee, SY; Houser, Jason
Subject: Re: Interview with New York Times

Adding Jason for his visibility.

Caroline, you and I can write the coordination piece related to the CT coordinator.

Jason and Alaina, can you take the second section?

Caroline and Nate, can you do CVE?

From: Henkels, Suzanne
Sent: Thursday, March 29, 2012 08:56 AM
To: Barry, Patrick
Cc: Duggan, Alaina; Simmons, Caroline; Snyder, Nathaniel; Lee, SY
Subject: RE: Interview with New York Times

Thanks again for this outline. Very helpful! Since you all have the most up-to-date info on the first three topic areas (**Organizational arrangements to improve coordination/ Specific measures to enhance domestic capabilities to detect and prevent terrorist attacks through/CVE)** Do you mind working to fill that in – im afraid we don't have the latest and greatest. We will fill in details for the last two topic areas – we have some recent talkers on cargo screening/scanning/Global Entry. Please let me know if you have any questions. Thank you!

From: Barry, Patrick
Sent: Wednesday, March 28, 2012 7:20 PM
To: Henkels, Suzanne
Cc: Duggan, Alaina; Simmons, Caroline; Snyder, Nathaniel
Subject: RE: Interview with New York Times

Hi Suzanne,

(b)(5)

Hope this helps!

Pat

From: Beers, Rand
Sent: Wednesday, March 28, 2012 5:33 PM
To: Cohen, John; Barry, Patrick
Subject: RE: Interview with New York Times

I would add and modify:

From: Cohen, John
Sent: Wednesday, March 28, 2012 2:30 PM
To: Barry, Patrick; Beers, Rand
Subject: Re: Interview with New York Times

(b)(5)

(b)(5)

John Cohen
Principal Deputy Counterterrorism Coordinator and Senior Advisor to the Secretary
United States Department of Homeland Security

From: Barry, Patrick
Sent: Wednesday, March 28, 2012 01:50 PM
To: Beers, Rand; Cohen, John
Subject: Fw: Interview with New York Times

First I've seen this.

From: Simmons, Caroline
Sent: Wednesday, March 28, 2012 01:46 PM
To: Barry, Patrick
Cc: Snyder, Nathaniel
Subject: Fw: Interview with New York Times

Thanks Nate. Looping Pat. Pat-assume you guys probably received a tasking on this from the front office? Did you already provide CT TPs? Nate and I will work on the CVE TPs but wanted to know if I should add CT ones too or if you did already? Thx!

From: Snyder, Nathaniel
Sent: Wednesday, March 28, 2012 12:57 PM
To: Henkels, Suzanne; Duggan, Alaina; caroline.simmon(b)(6)
Cc: Lee, SY
Subject: Re: Interview with New York Times

Adding Caroline... We can get moving on this quickly and may have to reach out to some other offices and components.

Nate Snyder
US Dept of Homeland Security
Cell: 202.590.0984
Email: (b)(6)
JWICS:
Message sent via BlackBerry

From: Henkels, Suzanne
Sent: Wednesday, March 28, 2012 12:46 PM
To: Duggan, Alaina; Snyder, Nathaniel
Cc: Lee, SY
Subject: Interview with New York Times

(b)(5)

(b)(5)

Sender: Henkels, Suzanne (b)(6)
(b)(6)

Recipient: "Simmons, Caroline (b)(6)
(b)(6)
"Barry, Patrick </O=
"Duggan, Alaina </O
"Snyder, Nathaniel <
(b)(6)
"Lee, SY </O=DHS
"Houser, Jason </O=

Sent Date: 2012/03/29 17:09:52

Delivered Date: 2012/03/29 17:09:54

From: Simmons, Caroline (b)(6)
(b)(6)
To: "Barry, Patrick < (b)(6)
(b)(6)
"Duggan, Alaina
(b)(6)
"Houser, Jason
(b)(6)
"Snyder, Nathar
(b)(6)
Subject: RE:
Date: 2012/03/29 15:47:07
Priority: Normal
Type: Note

Pat-

Revised bullets below. Nate, let me know if you have edits.

Overall Approach

- The White House CVE strategy was released in August, 2011. On December 8, 2011, the White House released the Strategic Implementation Plan (SIP) for the Administration's CVE Strategy. The SIP lists the current and future actions the USG will take in support of a locally-focused, community-based approach, in three broad areas: 1) Enhancing engagement and support to local communities; 2) Building government and law enforcement expertise; and 3) countering violent extremist propaganda. The SIP directly supports the DHS CVE Approach which was informed based on the recommendations from the HSAC CVE Working Group that were issued in August, 2010,

- DHS worked closely with the White House, NCTC, DOJ, and the FBI to develop the SIP, and will continue to work closely with these entities in implementing the priorities in the SIP.

  - ➢ DHS, NCTC, DOJ, and the FBI have formed a small working group to meet on a weekly basis to ensure the priorities in the SIP are implemented in a timely manner.
- In support of the SIP, DHS is working on the following key initiatives:

Training
DHS is working with state, local, tribal and federal partners to develop a CVE Curriculum for state, local, tribal, and federal law enforcement as well for use at academies.

- **DHS CVE Training for State and Local Law Enforcement** – The CVE Curriculum Pilot for State, Local and Tribal Law Enforcement was held in San Diego, CA on January 25-27, 2012. The LAPD and the National Consortium for Advanced Policing (NCAP) were successful in piloting the first working DRAFT of the curriculum to officers from San Diego PD, LAPD, LASD, San Diego Harbor PD, and other area law enforcement agencies (approximately 45 students). The curriculum will undergo further review and editing and further pilots will be conducted. The Major Cities Chiefs Association also passed a motion to adopt and implement the DHS CVE curriculum in their training academies.

- **DHS CVE Training for Federal Law Enforcement** On February 16, 2012, DHS/FLETC hosted a full day conference on CVE for their training staff in order to better understand the administration and DHS' CVE approach. DHS/I&A, S&T, CRCL, and NCTC provided presentations on the behaviors and indicators of violent extremism, and FLETC is working to incorporate their findings into their federal training curriculum.
- **DHS/DOJ SAR Training** - DHS and the Department of Justice have also trained over 190,000 frontline officers through the Nationwide Suspicious Activity Reporting (SAR) Initiative and hope to reach all of America's officers on the frontlines.
- **DHS CRCL Training** - To date, CRCL has already trained more than 2,100 police officers on ways to counter violent extremism in their own communities.
- **DHS Training for Correctional Facility Officers -** DHS Training for Correctional Facility Officers on CVE – DHS, in conjunction with the Interagency Threat Assessment and Coordination Group (ITACG) piloted a CVE training for Correctional Facility Officers on March 28, 2012 in Maryland.

International Partnerships

- **DHS Work with Europol** – DHS has worked closely Europol regarding: CVE information sharing initiatives; best practices at fusion centers; CVE training; increased information sharing between US fusion centers and EU fusion centers; and, improve knowledge of behaviors and indicators of violent extremism among DHS and European law enforcement.

    - DHS along with DOJ, NCTC, the FBI, and 5 State and Local Law Enforcement Representatives attended a Europol-U.S. CVE Conference at Europol Headquarters on March 19-21, 2012 to exchange case studies and behaviors and indicators on violent extremism, and CVE training curricula.

    - DHS received a briefing from Norwegians on the lessons learned from the Oslo shooting/bombing incident and DHS is working with Europol to develop a joint assessment on best practices on Fusion Centers.

    - DHS also received a briefing on the UK's CHANNEL/Prevent CVE intervention program and LAPD Deputy Chief Michael Downing presented the new State and Local Law Enforcement CVE Curriculum to Europol and EU partners.

From: Barry, Patrick
Sent: Thursday, March 29, 2012 3:13 PM
To: Duggan, Alaina; Simmons, Caroline; Houser, Jason; Snyder, Nathaniel
Subject: RE:

How's this? Jason and Nate, get me your stuff.

- DHS has established the "If You See Something, Say Something (TM)", a simple and effective program to raise public awareness of indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the authorities.

- Some of the most recent partnerships include the Super Bowl in Indianapolis, this was the second year in a row the Department partnered at the Super Bowl and for the security awareness brief provided a few days before the Super Bowl the Secretary traveled to Indianapolis to take part in it.

- In Florida we have partnered with the State along with many private sector partners to include the NBA at this year's All-Star Jam Session and with the Miami Heat and Orlando Magic, also, a few weeks ago we partnered with the Brickyard 400 in St. Petersburg.

From: Duggan, Alaina
Sent: Thursday, March 29, 2012 3:08 PM
To: Barry, Patrick; Simmons, Caroline; Houser, Jason; Snyder, Nathaniel
Subject: Re:

I'm no longer at a computer, I need someone who is in the office to help.

From: Barry, Patrick
Sent: Thursday, March 29, 2012 03:03 PM
To: Duggan, Alaina; Simmons, Caroline; Houser, Jason; Snyder, Nathaniel
Subject: RE:

I need Jason to get off his dug and provide input on the second category. Also, this is great, but probably too much. Can you scale it back to 2-3 sentences?

From: Duggan, Alaina
Sent: Thursday, March 29, 2012 2:56 PM
To: Simmons, Caroline; Houser, Jason; Snyder, Nathaniel; Barry, Patrick
Subject: Fw:

S4 language. Need anything else?

From: Alaina Duggan (b)(6)
Sent: Thursday, March 29, 2012 02:53 PM
To: Duggan, Alaina (b)(6)
Subject:

In July 2010 the Department launched the "If You See Something, Say Something (TM)" public awareness campaign - a simple and effective program to raise public awareness of indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities. The campaign was originally used by

New York's Metropolitan Transportation Authority (MTA), which has licensed the use of the slogan to DHS for anti-terrorism and anti-crime efforts. Since July of 2010 the Department has partnered with numerous state, local and private sector partners and continues to expand the campaign nationwide everyday.

The "If You See Something, Say Something™" campaign is being launched in conjunction with the rollout of the Nationwide Suspicious Activity Reporting Initiative (NS). The NSI is an administration-wide effort to develop, evaluate, and implement common processes and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism-related suspicious activities. Led by the Department of Justice, the NSI is implemented in partnership with state and local officials across the nation.Both the "If You See Something, Say Something™" campaign and the NSI underscore the concept that homeland security begins with *hometwon security* where an alert public plays a critical role in keeping our nation safe.

Some fo the most recent partnerships include the Super Bowl in Indianapolis, this was the second year in a row the Department partnered at the Super Bowl and for the security awareness brief provided a few days before the Super Bowl the Secretary traveld to Indianapolis to take part in it. In Florida we have partnered with the State along with many private sector partners to include the NBA at this year's All-Star Jam Session and with the Miami Heat and Orlando Majic, also, a few weeks ago we partnered with the Brickyard 400 in St. Petersbrg.

Sender: Simmons, Caroline (b)(6)
(b)(6)
Recipient: "Barry, Patrick < (b)(6)
"Duggan, Alaina
"Houser, Jason <
"Snyder, Nathani
(b)(6)
Sent Date: 2012/03/29 15:47:05
Delivered Date: 2012/03/29 15:47:07

Key Points on DHS Approach to Countering Violent Extremism

- We face a threat environment where violent extremism is neither constrained by international borders, nor limited to any single ideology.

- We know that foreign terrorist groups affiliated with al-Qa'ida, and individual terrorist leaders, are actively seeking to recruit and/or inspire individuals living in communities within the U.S. to carry out attacks against U.S. targets.

- However, this is not a phenomenon restricted solely to any one particular community and our efforts to counter violent extremism (CVE) are applicable to all ideologically motivated violence.

- DHS is a risk-based organization and we prioritize the utilization of resources based on what intelligence and analysis tells us presents the greatest threat to the Homeland.

- At DHS, we believe that local authorities and community members are best able to identify those individuals or groups residing within their communities exhibiting dangerous behaviors—and intervene—before they commit an act of violence.

- Everyone has a role to play in the safety and security of our nation, and time and again we see the advantage of public vigilance and cooperation, from information-sharing, community-oriented policing, and citizen awareness.

- Countering violent extremism is a shared responsibility, and DHS continues to work with a broad range of partners to gain a better understanding of the behaviors, tactics, and other indicators that could point to terrorist activity, and the best ways to mitigate or prevent that activity.

- The Department's efforts to counter violent extremism (CVE) are three-fold:
  - **Better understand the phenomenon of violent extremism**, and assess the threat it poses to the Nation as a whole, and within specific communities;
  - **Bolster efforts to address the dynamics of violent extremism** and strengthen relationships with those communities targeted for recruitment by violent extremists; and
  - **Expand support for information-driven, community-oriented policing efforts** that have proven effective in preventing violent crime across the Nation for decades.

Key Points on the Strategic Implementation Plan (SIP)

- The White House CVE strategy was released in August, 2011. On December 8, 2011, after 5 months of planning and consultation with interagency partners, the White House released the Strategic Implementation Plan (SIP) for the Administration's CVE Strategy.

- The SIP lists the current and future actions the USG will take in support of a locally-focused, community-based approach, in three broad areas:
  - **Enhancing Engagement with and support to local communities:** Our aims in engaging with communities to discuss violent extremism are to (1) share sound, meaningful, and timely information about the threat of radicalization to violence with a wide range of groups and organizations; (2) respond to concerns about government policies and actions; and (3) better understand how we can effectively support community-based solutions.
  - **Building Government and Law Enforcement Expertise:** We are building robust training programs to ensure that communities, government, and law enforcement receive accurate, intelligence-based information about the dynamics of violent extremism. Misinformation about the threat and poor training harms our security by sending stakeholders in the wrong direction and creating tensions with communities.
  - **Countering Violent Extremist Propaganda while Promoting our Ideals:** We will aggressively counter violent extremist ideologies – including on the Internet – by educating and empowering communities and promoting our ideals. In the case of our current priority, we will, through our words and deeds, rebut al-Qa'ida's lie that the United States is somehow at war with Islam.

- The SIP underscores the strength of community-based problem solving, local partnerships, and community-oriented policing. We are building our efforts from existing structures, while creating capacity to fill gaps as we implement programs.

IF ASKED:

What has DHS done to work across the homeland security enterprise to counter violent extremism and other threats?

- The Department has worked with state, local and tribal governments across the nation to incorporate homeland security and terrorism prevention efforts into day-to-day efforts to protect our communities from violent crime. These efforts include:
  - Establishing robust information sharing capabilities to provide state, local, and private sector authorities credible and specific, CLASSIFED and UNCLASSIFIED, threat-related information;
  - Building analytic capacity at the grass-roots level by supporting regional fusion centers so that national intelligence can be viewed within the context of local conditions thereby allowing state, local and tribal authorities to better assess the risk to their communities;
  - Providing frontline personnel with Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) training as to the behaviors and indicators associated with specific threats and terrorism-related crime so that our 800,000 state, local and tribal officers can better recognize terrorism-related suspicious activities; and
  - Raising public awareness to the behaviors and indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities., for example the Department's nationwide launch of the "If You See Something, Say Something ™" campaign.

How has the Department's CVE strategy aided in recent terrorist plots?

- If something is wrong, somebody locally will probably become aware. Our challenge is connecting those individuals with an appropriate response.
- A study from 2010 found that, between 1999 and 2009, more than 80 percent of foiled terrorist plots in the United States were thwarted because of observations from law enforcement or the general public.
- An examination of 86 terrorist cases in the U.S. from 1999 to 2009 by the Institute for Homeland Security Solutions shows that nearly half of those cases were related to al-Qaeda or al-Qaeda-inspired ideology, with the remainder due to a number of other violent extremist motivations
- By promoting public vigilance and community-policing efforts we are expanding our information sharing capabilities beyond local law enforcement, and by reporting suspicious behaviors we are able to intervene before there is an act of violence.

What is DHS doing to combat violent extremism?

- DHS CVE efforts include law enforcement training, community engagement, grievance resolution and enhanced efforts to understand the issue of violent extremism through S&T research and I&A analysis. These efforts are coordinated with the inter-agency and the NSS.
- DHS is expanding its support for local, information-driven community-oriented efforts to prevent violent crime and build safe, secure and resilient communities.
- Local community/government partnerships represent the best opportunity to identify and mitigate violence that may be ideologically motivated.

How is the federal government engaging frontline officers and community partners on countering violent extremism?

- Through our Office for Civil Rights and Civil Liberties (CRCL), DHS continues to educate tribal, state and local law enforcement on cultural awareness and how best to engage with communities.
- To date, CRCL has already trained more than 2,100 police officers on ways to counter violent extremism in their own communities.
- DHS and the Department of Justice have also trained over 198,690 frontline officers through the Nationwide Suspicious Activity Reporting (SAR) Initiative and hope to reach all of America's officers on the frontlines.
- In addition to these training initiatives, DOJ and DHS, under the Building Communities of Trust Guidance, have coordinated engage our state and local law enforcement and community partners to share best practices on forming working partnerships and community based solutions in meetings across the country.
- DHS is working with state, local, tribal and federal partners to develop a CVE Curriculum for state, local, tribal, and federal law enforcement as well for use at academics.

2 page draft document "The Role of Fusion Centers in Countering violent extremism, Fact Sheet"

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: Simmons, Caroline (b)(6)
GROUP/CN=RECIPI

To: "Meyer, Joel (b)(6)
"Snyder, Nathaniel </O=DHS ORG/OU=E2K3 ADMIN
(b)(5) (b)(6)

Subject: RE: CVE/AQAP

Date: 2012/03/27 13:09:06

Priority: Normal

Type: Note

Will check and get right back to you. Also, it might be useful to have this as a topic on the CVE agenda tomorrow so we can solicit input from all Components, would you be ok with that?

From: Meyer, Joel
Sent: Tuesday, March 27, 2012 11:23 AM
To: Simmons, Caroline; Snyder, Nathaniel
Subject: RE: CVE/AQAP

Thanks Caroline. Are there any other actions like the one you described in the last bullet that were undertaken specifically because of AQAP?

From: Simmons, Caroline
Sent: Tuesday, March 27, 2012 11:13 AM
To: Meyer, Joel; Snyder, Nathaniel
Subject: RE: CVE/AQAP

Hey Joel,
Below are some draft bullets. Nate, let me know if you have edits/additions. Thanks!

(b)(5)

(b)(5)

From: Meyer, Joel
Sent: Monday, March 26, 2012 3:58 PM
To: Snyder, Nathaniel; Simmons, Caroline
Subject: CVE/AQAP

Nate and Caroline, remember last week I spoke with both of you about any CVE actions the Dept's taken specifically related to AQAP? Can you send me bullets on this in the next day or two so Brian and I can incorporate it into the products for the AQAP Working Group?

Thanks a bunch,
Joel

Sender: Simmons, Caroline <(b)(6)
(b)(6)
Recipient: "Meyer, Joel (b)(6)
"Snyder, Nath
(b)(6)
Sent Oate: 2012/03/27 13:09:06

2 page draft document "The Role of Fusion Centers in Countering violent extremism, Fact Sheet"

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: Saupp, Kevin (b)(6)
To: "Snyder, Nathaniel (b)(6)
(b)(6)
Subject: RE: CVE panel
Date: 2012/03/23 22:11:06
Priority: Normal
Type: Note

thx - done

From: Snyder, Nathaniel
Sent: Friday, March 23, 2012 6:54 PM
To: Saupp, Kevin
Subject: RE: CVE panel

Hey Kevin – sorry for the delay here is the tweaked language… let me know if this works.

Thanks and have a good weekend!

This is the latest I have:

State and Local Support to Countering Violent Extremism Efforts

Session Description: Violent extremism (including HVE and other domestic violent extremism threats regardless of ideology) presents an enduring threat to public safety. Threat detection and identification remain core functions of fusion centers, accomplished primarily through the collection and analysis of suspicious activity reporting (SARs) generated through liaison, outreach, and educational programs. In December 2011, the White House released a Strategic Implementation Plan (SIP) to Counter Violent Extremism (CVE). The program describes CVE roles and functions at the Federal, State and local level. The SIP directs Federal Government activity in three specific areas: (1) enhancing engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals. State and local partners in fusion centers have further supported these efforts by empowering front-line personnel to understand local implications of national intelligence. This panel will discuss threat identification (HVE) and threat mitigation (CVE) policy and programs.

Takeaways:

- Learn about the Strategic Implementation Plan's key objectives and activities.

- Understand federal and local engagement activities and strategies that could help improve future products and provide actionable information for state and local law enforcement.

- Hear about locally-led fusion center efforts to identify and address Violent Extremism.
- COC 2: Analyze

From: Saupp, Kevin (b)(6)
Sent: Friday, March 23, 2012 05:33 PM
To: Trelles D'Alemberte; Diane Ragans
Cc: Snyder, Nathaniel <(b)(6)
Subject: CVE panel

Can you send the latest language we have for this?

Kevin Saupp Office (b)(6)
Branch Chief, Federal Interagency Coordination
Department of Homeland Security
Office of Intelligence and Analysis
State and Local Program Office

Sender: Saupp, Kevin <(b)(6)
Recipient: "Snyder, Nathaniel <(b)(6)
(b)(6)
Sent Date: 2012/03/23 22:09:01
Delivered Date: 2012/03/23 22:11:06

From: Saupp, Kevin </O=DHS ORG/OU=E2K3 ADMIN GROUP/CN=RECIPIENTS/CN=KEVIN.SAUPP>
To: "Snyder, Nathaniel </O=DHS ORG/OU=E2K3 ADMIN GROUP/CN=RECIPIENTS/CN=NATHANIEL.SNYDER>"
Subject: RE: Language
Date: 2012/03/23 17:32:56
Priority: Normal
Type: Note

Hey – that is too bureaucratic for the audience…. I think that is also an old version… let me ask Diane to send us the latest and we can work from that?

From: Snyder, Nathaniel
Sent: Friday, March 23, 2012 5:31 PM
To: Saupp, Kevin
Subject: RE: Language

Hey Kevin   for the call with Trevor, Heather and Oiane I went took a shot at revamping the language in this, that would still answer the concerns that Trevor brought up.

I would like to stay away from the confusion that is HVE vs. CVE. Instead I want to explain that HVE threat detection work and other threats (i.e. lone wolf, sovereign citizens, XRW, Eco-Terrorism) are all part of CVE. From our conversation on the phone today it sounds like some FCs are considering CVE as solely outreach and engagement; this is not the case. Instead CVE leverages multiple equities in a whole of government approach where FC's do play a big role and there is delineation between what front line officers do and the role of fusions centers. Also, if we talk about HVE's specifically we are only addressing part of the CVE issue.

(b)(5)

(b)(5)

Sent from blackberry

Sender: Saupp, Kevin (b)(6)

Recipient: "Snyder, Nathanie (b)(6)
(b)(6)

Sent Date: 2012/03/23 17:32:56

From: Saupp, Kevin <(b)(6)
To: "Snyder, Nathaniel <(b)(6)
(b)(6)
Subject: RE: Language
Date: 2012/03/23 13:18:11
Priority: Normal
Type: Note

Nate - call me if you want after, as there is a big issue with the FC role in CVE that we need to assist with and this helps address it

-----Original Message-----
From: Diane Ragans (b)(6)
Sent: Friday, March 23, 2012 1:16 PM
To: Snyder, Nathaniel
Cc: Saupp, Kevin
Subject: FW: Language

Nate - this is the proposed new session title and summary.

-----Original Message-----
From: Saupp, Kevin (b)(6)
Sent: Friday, March 23, 2012 12:17 PM
To: Diane Ragans
Subject: FW: Language

Is this different better than what we have?

-----Original Message-----
From: Wilson, Trevor
Sent: Friday, March 23, 2012 10:31 AM
To: Saupp, Kevin
Subject: Language

How's this Kevin: State and Local Support to Address Homegrown Violent Extremism

(b)(5)

(b)(5)

Sent from blackberry

Sender: Saupp, Kevin <(b)(6)

Recipient: "Snyder, Nathaniel <(b)(6)
(b)(6)

Sent Date: 2012/03/23 13:18:10

Delivered Date: 2012/03/23 13:18:11

The Role of Fusion Centers in Countering Violent Extremism

Fact Sheet

Overview

The threat posed by violent extremism is neither constrained by international borders nor limited to any single ideology. Groups and individuals inspired by a range of religious, political, or other ideological beliefs have promoted and used violence against the homeland. Increasingly sophisticated use of the Internet, mainstream and social media, and information technology by violent extremists adds an additional layer of complexity. To counter violent extremism, the U.S. Department of Homeland Security (DHS) is working with a broad range of partners, including state and major urban area fusion centers, to gain a better understanding of the behaviors, tactics, and other indicators that could point to potential terrorist activity within the United States and the best ways to mitigate or prevent that activity.

Fusion centers are state- and locally owned and operated assets that play a vital role in improving the nation's ability to safeguard the homeland. They are focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among federal; state, local, tribal, and territorial (SLTT); and private sector partners. As analytic hubs, fusion centers are uniquely situated to empower frontline personnel to understand the local implications of national intelligence by providing tailored local context to national threat information. Fusion centers support partners at all levels of government and within the Intelligence Community through a variety of activities ranging from improving analytic collaboration across jurisdictional boundaries to helping frontline personnel understand terrorist and criminal threats they could encounter in the field. For fusion centers to engage in effective and meaningful information sharing, they must do so in a manner that protects the privacy, civil rights, and civil liberties (P/CRCL) of all Americans. Fusion centers implement P/CRCL safeguards to protect constitutional rights and to ensure that they are addressing their ethical and legal obligations while engaged in the fusion process.

Fusion centers *play an important role in providing grassroots intelligence, analytic, and information sharing capabilities within the state and local environment to help identify and mitigate threats.*

This fact sheet provides an overview of the Department's approach to countering violent extremism and outlines the important role fusion centers play in providing grassroots intelligence, analytic, and information sharing capabilities within the state and local environment to help identify and mitigate threats.

Countering Violent Extremism

DHS's efforts to counter violent extremism are threefold:

- **Better understand the phenomenon of violent extremism**, and assess the threat it poses to the nation as a whole and within specific communities.
- **Bolster efforts to address the dynamics of violent extremism** and strengthen relationships with those communities targeted for recruitment by violent extremists.
- **Expand support for information-driven, community-oriented policing efforts** that have proved effective in preventing violent crime across the nation.

Support for Locally Based Approaches

In support of the *National Strategy on Empowering Local Partners to Prevent Violent Extremism*, the U.S. government has increased its support for locally focused, community-based approaches to countering violent extremism across three broad areas:

- **Enhancing Engagement With and Support to Local Communities:** Our aims in engaging with communities to discuss violent extremism are to (1) share sound, meaningful, and timely information about the threat of radicalization to violence with a wide range of groups and organizations; (2) respond to concerns about government policies and actions; and (3) better understand how we can effectively support community-based solutions.
- **Building Government and Law Enforcement Expertise:** We are building robust training programs to ensure that communities, the government, and law enforcement receive accurate, intelligence-based information about the dynamics of violent extremism. Misinformation about the threat and poor training harm our security by sending stakeholders in the wrong direction and creating tensions within communities.
- **Countering Violent Extremist Propaganda While Promoting Our Ideals:** We will aggressively counter violent extremist ideologies—including on the Internet—by educating and empowering communities and promoting our ideals. In the case of our current priority, we will, through our words and deeds, rebut al-Qa'ida's lie that the United States is somehow at war with Islam.

Role of Fusion Centers

In support of these overarching priorities, fusion centers play an important role in countering violent extremism efforts through their day-to-day activities, including gathering, analyzing, and sharing threat information. Therefore, the Department is continuing to support fusion centers as they share information and develop intelligence products that support their law enforcement customers' CVE efforts, including:

- Building grassroots intelligence and analytic capabilities within the state and local environment so state and local law enforcement partners can understand the local implications of national intelligence and providing tailored local context to national threat information.
- Based upon these analytic efforts, providing state and local law enforcement partners with timely, relevant, and accurate threat analysis, incorporating:
  - Trends or patterns in criminal and terrorist activities.
  - Identified vulnerabilities within a jurisdiction.
  - Indicators and warnings indicative of terrorism or violent crime.
  - How to report suspicious activities to the proper law enforcement authorities.
  - Recommendations for protective measures, preventive actions, or other threat mitigation activities.
- Sharing information with state and local decision makers to assist in the prioritization of resources to mitigate known threats.
- Sharing information with local law enforcement partners to help inform frontline officers in their community engagement efforts, including raising awareness of potential threats in their communities.
- Incorporating local law enforcement information in their analytic efforts, resulting in better-informed, relevant, and actionable products.
- Educating and informing local law enforcement on behaviors and indicators of potential threats, while ensuring the protection of the privacy, civil rights, and civil liberties of individuals and constitutionally protected activities.
- Leveraging Fusion Liaison Officer (FLO) programs to facilitate the exchange of information between fusion centers and their stakeholders, as FLO programs represent a valuable approach to building partnerships between fusion centers and local law enforcement community-policing efforts.

2 page draft document "The Role of Fusion Centers in Countering violent extremism"

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

2 page draft document "The Role of Fusion Centers in Countering violent extremism"

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: Diane Ragans (b)(6)
To: "Snyder, Nathaniel </(b)(6)
(b)(6)
"Parker, Bradford </C
(b)(6)
"Saupp, Kevin </O=D
CC: "Schapiro, Amy <(b)(6)
(b)(6)
"Duggan, Alaina
(b)(6)
"Simmons, Caroli
(b)(6)
Subject: Re: NFC Conf CVE panels
Date: 2012/03/16 21:50:29
Type: Note

Thanks Nate. I hope your trip goes well next week.
Sent from my BlackBerry Wireless Handheld

From: Snyder, Nathaniel (b)(6)
Sent: Friday, March 16, 2012 09:29 PM
To: Diane Ragans; Parker, Bradford (b)(6) Saupp, Kevin
<(b)(6)
Cc: Schapiro, Amy (b)(6) Duggan, Alaina
(b)(6); Simmons, Caroline <(b)(6)
Subject: RE: NFC Conf CVE panels

Both times work for me.

Will work on a bio.

Thanks,

-Nate

From: Diane Ragans (b)(6)
Sent: Friday, March 16, 2012 1:09 PM
To: Snyder, Nathaniel; Parker, Bradford; Saupp, Kevin
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline
Subject: RE: NFC Conf CVE panels

I think Friday next week would work fine for a call. I just spoke to one of the panelists, Heather Perez, and she advised she would like to use a PPT so I think it would be great to run through the items I listed below as well as any others identified so the session runs smoothly.

How does a call on Friday afternoon, 3/23 look for you – maybe at 1:00 or 2:00 PM (ET)? Having it later in the day will accommodate Christa Burch, our West Coast panelist. I will send out an outlook appt. upon hearing back on your preference.

One last item – could you please forward me a brief bio at your earliest convenience?

Thanks much! Diane

From: Snyder, Nathaniel (b)(6)
Sent: Friday, March 16, 2012 12:57 PM
To: Diane Ragans; Parker, Bradford; Saupp, Kevin
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline
Subject: RE: NFC Conf CVE panels

Diane – thank you, this is very helpful. A few of us will be in Europe next week; panel participants included. If it is not too late, Friday next week could work.

Thanks again,

-Nate

From: Diane Ragans (b)(6)
Sent: Friday, March 16, 2012 12:53 PM
To: Snyder, Nathaniel; Parker, Bradford; Saupp, Kevin
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline
Subject: RE: NFC Conf CVE panels

Hi Nate.

The session titled State and Local Support to Counter Violent Extremism (CVE) will occur on **Wednesday, April 4 from 4:15 - 5:30 PM**. I expect you've already seen it, but here is the write-up for the session:

State and Local Support to Counter Violent Extremism (CVE)

Session Description: Last December, the White House released its Strategic Implementation Plan to Counter Violent Extremism. The program describes the CVE roles and functions at the Federal, State and local level. The SIP directs Federal Government activity in three specific areas: enhancing engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals. Local officials and authorities in many cities have begun to implement training and outreach efforts tailored for their specific communities.

Takeaways:

- Learn about the Strategic Implementation Plan's key objectives and activities.
- Understand federal engagement activities and strategies.
- Hear lessons learned from long standing programs and introduce new strategies to engage these communities.
- COC 2: Analyze

I would be happy to arrange for a conference call with all participants next week to discuss flow of the session, topics each will cover, order of the speakers, etc. Do you have a preference for the date or time? As the call organizer, the only day I cannot do it is on Tuesday, 3/20. I am already scheduled for an all day meeting. I look forward to hearing back from you.

Regards, Diane

Diane G. Ragans
Institute for Intergovernmental Research
(b)(6)

From: Saupp, Kevin (b)(6)
Sent: Friday, March 16, 2012 11:31 AM
To: Snyder, Nathaniel; Parker, Bradford
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline; Diane Ragans
Subject: RE: NFC Conf CVE panels

All, I expect believe the full agenda will be available next week on the website.

From: Snyder, Nathaniel
Sent: Friday, March 16, 2012 10:58 AM
To: Parker, Bradford; Saupp, Kevin
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline; (b)(6)
Subject: RE: NFC Conf CVE panels

This looks good.

Is there an overall agenda that can be shared? It would be good to see when this panel is and what proceeds and follows it.

Thanks,

-Nate

From: Parker, Bradford
Sent: Thursday, March 15, 2012 3:29 PM
To: Saupp, Kevin; Snyder, Nathaniel
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline; (b)(6)
Subject: RE: NFC Conf CVE panels

All,

Here goes- last second change but hopefully won't be too much of an issue:

Moderator: Nate Snyder
Seamus Hughes, NCTC
(b)(7)(C)
Heather Perez, CFIX
(b)(7)(C)

(b)(7)(C)

Thanks,

Bradford J. Parker
Senior Intelligence Officer
Homegrown Violent Extremism Branch (HVEB)
Homeland Counterterrorism Division (HCTD)
Department of Homeland Security
Office of Intelligence and Analysis
COMM(b)(7)(C)
NSTS:

From: Saupp, Kevin
Sent: Thursday, March 15, 2012 11:44 AM
To: Snyder, Nathaniel
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline; Parker, Bradford;(b)(6)
Subject: Re: NFC Conf CVE panels

Nate, Brad Parker is running point and would have that info - Brad?

From: Snyder, Nathaniel
Sent: Thursday, March 15, 2012 10:39 AM
To: Saupp, Kevin
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline
Subject: NFC Conf CVE panels

Hey Kevin – I wanted to check with you on the CVE panels.

Do you have the details on who is doing them and an agenda you can share?

Also, is there a plan to do a dry-run before the conference?

Want to ensure that both panels are as tight as they can be and that we are prepared to answer questions.

This is a huge opportunity.

I am hoping to finalize my travel plans tomorrow; I may not be able to stay for the full conference.

Thanks,

-Nate

Nate Snyder

(b)(6)

(b)(6)

Sender: Diane Ragans (b)(6)

Recipient: "Snyder, Nathaniel (b)(6)
(b)(6)
"Parker, Bradford <
(b)(6)
"Saupp, Kevin </O
(b)(6)
"Schapiro, Amy </(
(b)(6)
"Duggan, Alaina </
(b)(6)
"Simmons, Caroline
(b)(6)

Sent Date: 2012/03/16 21:50:18

Delivered Date: 2012/03/16 21:50:29

From: Trelles D'Alemberte <(b)(6)
To: "Diane Ragans (b)(6)
"Saupp, Kevin
(b)(6)
"Snyder, Nath
(b)(6)
"Parker, Bradf
(b)(6)
CC: "Schapiro, Amy <(b)(6)
(b)(6)
"Duggan, Alaina <
(b)(6)
"Simmons, Carolin
(b)(6)
Subject: RE: NFC Conf CVE panels
Date: 2012/03/16 13:40:15
Type: Note

Yes it is possible and I will make this update.

Thank you,
Trelles

From: Diane Ragans
Sent: Friday, March 16, 2012 1:11 PM
To: 'Saupp, Kevin'; 'Snyder, Nathaniel'; 'Parker, Bradford'
Cc: 'Schapiro, Amy'; 'Duggan, Alaina'; 'Simmons, Caroline'; Trelles D'Alemberte
Subject: RE: NFC Conf CVE panels

Kevin – Trelles can best respond to your question.

From: Saupp, Kevin (b)(6)
Sent: Friday, March 16, 2012 1:09 PM
To: Diane Ragans; Snyder, Nathaniel; Parker, Bradford
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline
Subject: RE: NFC Conf CVE panels

Diane – if we can, I'd like to update the description per the below in red to more accurately reflect the panelists. Is this possible?

From: Diane Ragans (b)(6)
Sent: Friday, March 16, 2012 12:53 PM
To: Snyder, Nathaniel; Parker, Bradford; Saupp, Kevin
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline
Subject: RE: NFC Conf CVE panels

Hi Nate.

(b)(5)

Regards, Diane

Diane G. Ragans
Institute far Intergovernmental Research
(b)(6)

From: Saupp, Kevin (b)(6)
Sent: Friday, March 16, 2012 11:31 AM
To: Snyder, Nathaniel; Parker, Bradford
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline; Diane Ragans
Subject: RE: NFC Conf CVE panels

All, I expect believe the full agenda will be available next week on the website.

From: Snyder, Nathaniel
Sent: Friday, March 16, 2012 10:58 AM
To: Parker, Bradford; Saupp, Kevin

Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline; (b)(6)
Subject: RE: NFC Conf CVE panels

This looks good.

Is there an overall agenda that can be shared? It would be good to see when this panel is and what proceeds and follows it.

Thanks,

-Nate

From: Parker, Bradford
Sent: Thursday, March 15, 2012 3:29 PM
To: Saupp, Kevin; Snyder, Nathaniel
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline; (b)(6)
Subject: RE: NFC Conf CVE panels

All,

Here goes- last second change but hopefully won't be too much of an issue:

Moderator: Nate Snyder
Seamus Hughes, NCTC
(b)(7)(C)

Thanks,

Bradford J. Parker
Senior Intelligence Officer
Homegrown Violent Extremism Branch (HVEB)
Homeland Counterterrorism Division (HCTD)
Department of Homeland Security
Office of Intelligence and Analysis
COMM (b)(6)
NSTS:

From: Saupp, Kevin
Sent: Thursday, March 15, 2012 11:44 AM
To: Snyder, Nathaniel
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline; Parker, Bradford; (b)(6)
Subject: Re: NFC Conf CVE panels

Nate, Brad Parker is running point and would have that info - Brad?

From: Snyder, Nathaniel
Sent: Thursday, March 15, 2012 10:39 AM
To: Saupp, Kevin
Cc: Schapiro, Amy; Duggan, Alaina; Simmons, Caroline
Subject: NFC Conf CVE panels

Hey Kevin – I wanted to check with you on the CVE panels.

Do you have the details on who is doing them and an agenda you can share?

Also, is there a plan to do a dry-run before the conference?

Want to ensure that both panels are as tight as they can be and that we are prepared to answer questions.

This is a huge opportunity.

I am hoping to finalize my travel plans tomorrow; I may not be able to stay for the full conference.

Thanks,

-Nate

Nate Snyder

(b)(6)

Sender: Trelles D'Alemberte (b)(6)
Recipient: "Diane Ragans (b)(6)
"Saupp, Kevin
(b)(6)
"Snyder, Natha
(b)(6)
"Parker, Bradfo
(b)(6)
"Schapiro, Amy
(b)(6)
"Duggan, Alain
(b)(6)
"Simmons, Car
(b)(6)
Sent Date: 2012/03/16 13:39:59
Delivered Date: 2012/03/16 13:40:15

3 page draft document "Key approach to countering violent extremism" final document released in full

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: (b)(6)
To: "Snyder, Nathaniel < (b)(6)
(b)(6)
CC: "Simmons, Caroline < (b)(6)
(b)(6)
Subject: I&A Panel
Date: 2012/03/15 08:34:19
Type: Note

Morning Nate,

It seems that I&A heard us talking yesterday. This is the updated description I got from them. I'm about to tell them that Seamus Hughes will be attending for us and doing the panel with you.

(b)(5)

Bridget E. Matty
Countering Violent Extremism (CVE) Group
National Counterterrorism Center
(b)(6)

Sender: (b)(6)
Recipient: "Snyder, Nathaniel < (b)(6)
(b)(6)
"Simmons, Caroline <
(b)(6)
Sent Date: 2012/03/15 08:34:19

2 page draft document "Scope for cyber awareness workshop"

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

5 page draft "DHS countering violent extremism approach overview"

Page 1 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 4 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 5 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

3 page draft "key points on approach to countering violent extremism"

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

3 page draft "Key points on DHS approach to countering violent extremism"

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

3 page draft "Key points on DHS approach to countering violent extremism"

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

KEY MESSAGES:

Organization and Planning to Improve Counterterrorism Coordination

- Following the attempted attack on December 25, 2009, I directed Rand Beers to be the Department's Coordinator for Counterterrorism in order to better coordinate counterterrorism activities across the Department's directorates, components, and offices related to detection, prevention, response to, and recovery from acts of terrorism.
- This includes syncing intelligence with operators in relevant components; breaking down obstacles that prevent components from responding to threats with appropriate countermeasures; and identifying systemic challenges afflicting the department.
- The CT Coordinator also chairs the Counterterrorism Advisory Board (CTAB), which serves as a consistent, high-level forum for coordination on counterterrorism among DHS components.
- The CTAB brings together the intelligence, operational and policy-making elements within DHS headquarters and its components.
- The CTAB has been an integral coordinating body that has assisted in responding to numerous threat streams in the past year. For example, the CTAB was the main body coordinating all of the Department's countermeasures in the lead up to the 10th Anniversary of 9/11. The CTAB also successfully coordinated the Department's countermeasures during the 2011 Holiday period and it continues to engage in intelligence review and operational coordination regarding potential threat streams.

Enhanced Domestic Capabilities to Detect and Prevent Terrorist Attacks

- **Information Sharing**
  - DHS has more efficiently and effectively disseminated information to State and Local Law Enforcement, through Joint Intelligence Bulletins (JIBS), Intelligence Briefings, and Outreach to Federal, State, Local, Private Sector, and other community partners on the new National Terrorism Alert System (NTAS).
- **Support for State and Local Law Enforcement**
  - DHS has helped establish a more robust grassroots analytic capability at fusion centers by ensuring that national intelligence is analyzed and applied to a local context to enable better operational planning for state and local law enforcement. DHS has also enhanced law enforcement and intelligence community information to support investigations, and locally-focused analytical work.
- **Standardizing Training for Officers to Report Suspicious Activities**
  - In March 2010, the Nationwide SAR Initiative (NSI) Program Management Office (PMO) was established within the U.S. Department of Justice (DOJ), Bureau of Justice Assistance, and is an interagency office composed of representatives from DOJ, DHS, FBI, and the PM-ISE.
  - DHS and DOJ have trained over 190,000 frontline officers through the SAR Initiative and hope to reach all of America's officers on the frontlines.
- **Raising Community Awareness**
  - DHS has established the "If You See Something, Say Something (TM)", campaign in conjunction with the Department of Justice's Nationwide Suspicious Activity Reporting Initiative to raise public awareness of indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the authorities.

- Recent expansions of the "If You See Something, Say Something™" campaign include partnerships with numerous sports teams and leagues, transportation agencies, private sector partners, states, municipalities, and colleges and universities.
- DHS also unveiled new Public Service Announcements which have been distributed to television and radio stations across the country.

- **NYPD Intelligence Division**
  - This falls under the jurisdiction of the New York Police Department and I would encourage you to direct any questions on this program to the NYPD

<u>Efforts to Counter Violent Extremism (CVE)</u>

- **Overall CVE Approach**
  - The White House CVE strategy was released in August, 2011. On December 8, 2011, the White House released the Strategic Implementation Plan (SIP) for the Administration's CVE Strategy. The SIP lists the current and future actions the USG will take in support of a locally-focused, community-based approach, in three broad areas:
    - Enhancing engagement and support to local communities
    - Building government and law enforcement expertise
    - Countering violent extremist propaganda
  - The SIP directly supports the DHS CVE Approach which was informed based on the recommendations from the HSAC CVE Working Group that were issued in August, 2010
  - DHS worked closely with the White House, NCTC, DOJ, and the FBI to develop the SIP, and will continue to work closely with these entities in implementing the priorities in the SIP. In support of the SIP, DHS is working on the following key initiatives:
  - **CVE Training**
    - **Overall Training -** DHS is working with state, local, tribal and federal partners to develop a CVE Curriculum for state, local, tribal, and federal law enforcement as well for use at academies.
    - **DHS CVE Training for State and Local Law Enforcement –** In January, DHS, in conjunction with the LAPD and the National Consortium for Advanced Policing (NCAP) held the CVE Curriculum Pilot for State, Local and Tribal Law Enforcement in San Diego, Calif. for officers from San Diego PD, LAPD, LASD, San Diego Harbor PD, and other area law enforcement agencies (approximately 45 students). The curriculum will undergo further review and editing and further pilots will be conducted. The Major Cities Chiefs Association also passed a motion to adopt and implement the DHS CVE curriculum in their training academies.
    - **DHS CVE Training for Federal Law Enforcement –** On February 16, 2012, DHS/FLETC hosted a full day conference on CVE for their training staff in order to better understand the administration and DHS' CVE approach.
    - **DHS CRCL Training** - To date, CRCL has already trained more than 2,100 police officers on ways to counter violent extremism in their own communities.
    - **DHS Training for Correctional Facility Officers -** DHS, in conjunction with the Interagency Threat Assessment and Coordination Group (ITACG) piloted a CVE training for Correctional Facility Officers on March 28, 2012 in Maryland.
  - **International Partnerships**

  - **DHS Work with Europol** – DHS is working closely with Europol to share information best practices at fusion centers; CVE training; increased information sharing between US fusion centers and EU fusion centers; and, improved knowledge of behaviors and indicators of violent extremism among DHS and European law enforcement.

<u>Enhanced screening of those individuals and cargo entering the United States</u>

- **US-VISIT**
  - ➢ US-VISIT supports DHS's mission to protect our nation by providing biometric identification services to federal, state, and local government decision makers to help them accurately identify the people they encounter, and determine whether those people pose a risk to the United States.
  - ➢ DHS's use of biometrics under the US-VISIT program is a powerful tool in preventing identity fraud and ensuring that DHS is able to rapidly identify criminals and immigration violators who apply for visas, try to enter the United States, or apply for immigration benefits.
  - ➢ US-VISIT also analyzes biographical entry and exit records stored in its Arrival and Departure Information System to further support DHS's ability to identify international travelers who have remained in the United States beyond their periods of admission.

- **100% Scanning Mandate (Maritime)**
  - ➢ 100 percent cargo scanning mandate poses significant operational, diplomatic, financial, and technical challenges.
  - ➢ The Administration is taking concrete steps to strengthen maritime transportation security. DHS is addressing this issue comprehensively through a risk- and technology-based approach by mitigating threats across all potential pathways and evaluating vulnerability across a complex system.
  - ➢ We're continuing research and development work to address some of the limitations inherent in available technology and to explore innovative next-generation capabilities.
    - Mobile scanning systems and technologies with enhanced penetration capabilities to strengthen the ability to find illicit materials in very dense cargo.
    - Technologies that can automatically detect and analyze suspicious anomalies within cargo containers, mitigating the need for more time-consuming and challenging manual inspections.

- **100% Screening Mandate (Air)**
  - ➢ With cargo transported on passenger aircraft from over 350 domestic airports and 200 international airports with flights to the United States, the scope and nature of the 9/11 Act's 100-percent screening requirement presents significant challenges.
  - ➢ Today, 100 percent of high risk cargo on international flights bound for the United States is screened and is prohibited from being transported on passenger aircraft.
  - ➢ TSA will work with industry to leverage and enhance ongoing programs including the collection of pre-departure data for international inbound cargo, and certify foreign aviation security programs that are commensurate with TSA standards through TSA's National Cargo Security Program recognition process.

- Earlier this year, TSA requested feedback from the airline industry on proposed enhanced security measures for screening 100 percent of air cargo on international inbound passenger aircraft.
- The proposal includes a potential implementation date of Dec. 1, 2012 to mandate screening 100 percent screening. TSA is reviewing industry comments prior to determining whether to move forward with this proposal, which builds additional procedures into the prescreening and analysis process.

- **Global Supply Chain**
  - **How is the US targeting a response to highly vulnerable areas?**
    - The United States has three priorities across all areas of the global supply chain: preventing terrorists from exploiting the supply chain to plan and execute attacks, protecting transportation hubs from attacks and disruptions, and building the resilience of the global supply chain to ensure that if something does happen, the supply chain can recover quickly.
    - We are working to raise international screening standards by developing and expanding upon risk-based targeting that customs agencies use to focus their resources on the most dangerous shipments.
    - We are working to develop and deploy technologies that can better track and detect illicit goods, as well as improve the capacities of countries around the world to ensure that customs agencies are able to do their jobs everywhere along the global supply chain.
    - In partnership with the World Customs Organization (WCO), INTERPOL, the UN Office of Drugs and Crime in 2010, and over 89 participating nations and organizations, we are enlisting other nations, international bodies and the private sector to increase the security of the global supply chain through a series of initiatives to make the system stronger, smarter and more resilient.

  - **You say that Global Shield has been successful in interdicting suspicious shipments. What types of materials have been seized?**
    - Since the program commenced on Nov. 1, 2010, Global Shield participants conducted and reported a total of 36 seizures of precursor chemicals from Afghanistan, Kyrgyzstan, Tajikistan, Pakistan, Kenya, Uganda and Kazakhstan. As of March 2012, Program Global Shield has accounted for seizures of chemical precursors totaling over 62 metric tons and 35 arrests related to the illicit diversion of these chemicals.
    - These precursor chemicals are increasingly being used to create improvised explosive devices (IEDs).
    - To put this in perspective, on July 7, 2005, more than 50 people were killed, and more than 700 were injured when the London bombers used four bombs that each contained approximately 4.5 kilograms of peroxide-based explosives - three on London Underground trains and a fourth bomb exploding in a double-decker bus.
    - Due to its success, on March 22, 2011, the WCO Enforcement Committee endorsed a proposal to make Global Shield a long-term program within the WCO; enabling police and customs administrations to continue multilateral efforts to combat the illicit trafficking and diversion of bomb-making materials by terrorist and other criminal organizations.

Screening for air travel within the United States

- **Secure Flight**
  - As of November 23, 2010, 100 percent of domestic and international airlines with flights into, out of and within the United States are now being checked against government watch lists through TSA's Secure Flight program fulfilling a key 9/11 Commission recommendation a month ahead of schedule.
  - Currently, Secure Flight is conducting watch list matching for 100 percent of passengers who fly into, out of and within the U.S. Secure Flight is a phased-in program and addressing routes that overfly the United States is the next phase in its implementation.
  - TSA continues to work with our international and industry partners to ensure the successful implementation of vetting overflights and is carefully considering all privacy, policy and technical implications.
  - TSA works closely with our international partners to share information and the latest intelligence. TSA maintains the right to divert any flight that overflies the U.S. and has the potential to cause harm within the U.S.
  - Secure Flight helps prevent the misidentification of passengers who have similar names to individuals on the watch list and better identify individuals who may pose a known or suspected threat to aviation.

- **TSA PreCheck**
  - The TSA PreCheck initiative implements a key component of the agency's intelligence-driven, risk-based approach to security.
  - This program is designed to enhance security by placing more focus on pre-screening individuals who volunteer information about themselves prior to flying in order to potentially expedite the travel experience.
  - As TSA moves further away from a one-size-fits-all approach, our ultimate goal is to provide the most effective security in the most efficient way possible.
  - These are clear examples of TSA's commitment to focusing its attention and resources on those who present the greatest risk, thereby improving security and the travel experience for passengers.

- **What is TSA doing to become more risk-based in their screening at airports?**
  - TSA will continue to incorporate random and unpredictable security measures throughout the airport and no individual will be guaranteed expedited screening.
  - Physical screening is just one layer of aviation security. Other layers include intelligence gathering and analysis, explosive-detection canine teams, federal air marshals, closed-circuit television monitoring and behavior detection officers.
  - There is no single profile of a would-be terrorist. Research and experience has shown that an individual's or a group's ethnic, religious, or cultural background does not explain why a small number of individuals choose to pursue violence.
  - We therefore have no interest in policing beliefs or in profiling based on factors like religion or ethnicity. These practices are not only illegal, they are also ineffective.
  - We are working with a broad range of partners to gain a better understanding of the behaviors, tactics, and other indicators that could point to terrorist activity, and the best ways to mitigate or prevent that activity.

- Over the past ten years, DHS / TSA have strengthened security through a layered, risk-based system, including full implementation of Secure Flight, under which DHS prescreens 100 percent of passengers on flights flying to, from, or within the U.S. against government watchlists.

- **What's new about the final rule to expand and make the Global Entry program permanent? Hasn't Global Entry been running for awhile?**
  - The Final Rule establishes Global Entry as a permanent voluntary program. The Global Entry program, like the Global Entry pilot, will facilitate the movement of pre-approved, low-risk air travelers arriving in the United States.
  - Under this Final Rule, current participants in the pilot program will automatically be enrolled in the permanent Global Entry program for five years from the date of enrollment in the pilot program. Participation in Global Entry will continue to be voluntary.
  - CBP anticipates that the Global Entry program will eventually be expanded to operate at most major international airport locations within the United States. CBP will announce new airports in a Federal Register notice and on the website www.globalentry.gov
  - Age eligibility criteria have changed. All references to the age limit of 14 are removed. This change will allow more families to enjoy the benefits of the program. Persons under the age of 18 who meet the general eligibility criteria and have the consent of a parent or legal guardian will be eligible to participate in Global Entry.

- **How will the U.S. government make sure that travelers enrolled in Global Entry are low-risk?**
  - First, travelers must be pre-approved before they can participate in the pilot project. All applicants will undergo a rigorous background check, including a fingerprint check, and will be interviewed by a CBP officer before they are enrolled in the Global Entry pilot. Second, automated enforcement checks will take place every time the member uses the Global Entry kiosk to enter the United States. Third, any member of Global Entry may be referred for further examination at any time when entering the United States.

- **What measures does DHS take to ensure that American citizens' civil rights and civil liberties are protected?**
  - DHS's Office for Civil Rights and Civil Liberties plays a key role in the Department's mission to secure the nation while preserving individual freedoms of Americans.
  - DHS builds privacy and civil rights and civil liberties protections into its operations, policies and technology deployments from the outset of their development.
  - The DHS Privacy Office partners with every component of the Department to assess programs, systems, technologies or rule-makings for privacy risks, and recommends privacy protections and methods for handling personally identifiable information.

3 page draft "Parameter language"

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

NATIONAL SECURITY STAFF

Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States

As a government, we are working to prevent all types of extremism that leads to violence, regardless of who inspires it. At the same time, countering al-Qa'ida's violent ideology is one part of our comprehensive strategy to defeat al-Qa'ida. Over the past 2½ years, more key al-Qa'ida leaders—including Usama bin Laden—have been eliminated in rapid succession than at any time since the September 11 attacks. We have strengthened homeland security and improved information sharing. Thanks to coordinated intelligence and law enforcement, numerous terrorist plots have been thwarted, saving many American lives.

—*President Barack Obama, August 2011*

Law enforcement and government officials for decades have understood the critical importance of building relationships, based on trust, with the communities they serve. Partnerships are vital to address a range of challenges and must have as their foundation a genuine commitment on the part of law enforcement and government to address community needs and concerns, including protecting rights and public safety. In our efforts to counter violent extremism, we will rely on existing partnerships that communities have forged with Federal, State, and local government agencies. This reliance, however, must not change the nature or purpose of existing relationships. In many instances, our partnerships and related activities were not created for national security purposes but nonetheless have an indirect impact on countering violent extremism (CVE).

At the same time, this Strategic Implementation Plan (SIP) also includes activities, some of them relatively new, that are designed specifically to counter violent extremism. Where this is the case, we have made it clear. It is important that both types of activities be supported and coordinated appropriately at the local level.

Background

The President in August 2011 signed the *National Strategy for Empowering Local Partners to Prevent Violent Extremism in the United States* (National Strategy for Empowering Local Partners), which outlines our community-based approach and the Federal Government's role in empowering local stakeholders to build resilience against violent extremism.[1] It recognizes that, as the National Security Strategy from May 2010 highlights, "our best defenses against this threat are well informed and equipped families, local communities, and institutions." To support our overarching goal of preventing violent extremists and their supporters from inspiring, radicalizing, financing, or recruiting individuals or groups in the

[1] The National Strategy for Empowering Local Partners defines violent extremists as "individuals who support or commit ideologically motivated violence to further political goals."

United States to commit acts of violence, the Federal Government is focused on three core areas of activity: (1) enhancing engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals.

The SIP details how we are implementing the National Strategy for Empowering Local Partners. It explains our core objectives and sub-objectives; describes how activities by departments and agencies are aligned with these; lists planned activities that address gaps and expand efforts; and assigns Federal Government leads and partners for various actions. The SIP provides a blueprint for how we will build community resilience against violent extremism.[2] It does not address our overseas CVE efforts, other than ensuring we coordinate domestic and international activities.

Although the SIP will be applied to prevent all forms of violent extremism, we will prioritize preventing violent extremism and terrorism that is inspired by al-Qa'ida and its affiliates and adherents, which the 2010 National Security Strategy, the 2011 National Strategy for Counterterrorism, and the National Strategy for Empowering Local Partners identify as the preeminent security threats to our country. This is, however, a matter of emphasis and prioritization, and does not entail ignoring other forms of violent extremism. As the July 2011 terrorist attack in Norway underscored, free societies face threats from a range of violent extremists.

As the activities described in the SIP are executed, there will be major and long-lasting impacts:

- There will be platforms throughout the country for including communities that may be targeted by violent extremists for recruitment and radicalization into ongoing Federal, State, and local engagement efforts;
- The Federal Government will support that engagement through a task force of senior officials from across the government;
- Community-led efforts to build resilience to violent extremism will be supported;
- Analysis will increase in depth and relevance, and will be shared with those assessed to need it, including Governor-appointed Homeland Security Advisors, Major Cities Chiefs, Mayors' Offices, and local partners;
- Training for Federal, State, tribal, and local government and law enforcement officials on community resilience, CVE, and cultural competence will improve, and that training will meet rigorous professional standards; and
- Local partners, including government officials and community leaders, will better understand the threat of violent extremism and how they can work together to prevent it.

[2] The concept of "resilience" has applied to a range of areas such as emergency preparedness and critical infrastructure protection (e.g., the ability of financial markets, power suppliers, and telecommunications companies to withstand an attack or disaster and resume operations rapidly.) The National Security Strategy emphasized the importance of including individuals and communities in our approach to enhancing resilience. Both the National Strategy for Empowering Local Partners and the 2011 National Strategy for Counterterrorism expanded this concept to CVE, the latter explicitly stating, "We are working to bring to bear many of these capabilities to build resilience within our communities here at home against al-Qa'ida inspired radicalization, recruitment, and mobilization to violence."

The SIP outlines ongoing, as well as planned, activities to counter violent extremism, which will be accomplished through existing funding and by prioritizing within the resources available to relevant departments and agencies. Some of these activities are specific to CVE, while others address broader non-security policy objectives but may have an indirect effect on countering radicalization to violence. Because our efforts are threaded across a range of different missions, such as training, outreach, and international exchanges, the execution of the SIP will be impacted by funding for both security and non-security related activities.

Process for Developing the SIP

The Obama Administration continues to prioritize and stress the critical importance of CVE in the Homeland. Given the complexities of addressing this threat and the uniqueness of the operating environment in the United States, the Administration recognizes the potential to do more harm than good if our Nation's approach and actions are not dutifully considered and deliberated. Throughout this process, careful consideration was given to the rule of law and constitutional principles, particularly those that address civil rights and civil liberties. With those principles in mind, we noted that departments and agencies with domestically focused mandates have an array of tools and capabilities that can be leveraged to prevent violent extremism, though some have limited experience in the national security arena. This necessitated a deliberative and carefully calibrated approach with an extensive evaluative period to fully address their potential roles and participation, which for some entailed thinking outside their traditional mandates and areas of work.

After assessing how individuals are radicalized and recruited to violence in the United States, the Administration established an accelerated process, led by the National Security Staff (NSS), to develop the National Strategy for Empowering Local Partners and the SIP. An Interagency Policy Committee (IPC) on countering and preventing violent extremism in the United States was established—with Assistant and Deputy Assistant Secretary-level representatives from across government—to consider roles and responsibilities, potential activities, guiding principles, and how best to coordinate and synchronize our efforts. The IPC, with support from specialist sub-IPCs, drafted our first national strategy on preventing violent extremism in the United States, which was approved by Deputies from the various departments and agencies and signed by the President.

- The following departments and agencies were involved in the deliberations and approval process: the Departments of State (State), the Treasury, Defense (DOD), Justice (DOJ), Commerce, Labor, Health and Human Services (HHS), Education (EDU), Veterans Affairs, and Homeland Security (DHS), as well as the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC).

To develop the SIP, the NSS tasked NCTC with coordinating the first comprehensive baseline of activities across the United States Government related to countering and preventing violent extremism in the United States, which constitutes the ongoing activities outlined in the SIP. This included CVE-specific initiatives, as well as activities that were not developed for CVE purposes, but nonetheless may indirectly contribute to the overall goals of the National Strategy for Empowering Local Partners. These activities were aligned with objectives and sub-objectives—based on the strategy and approved by the IPC—to

assess our overall effort and identify gaps. The IPC then considered ongoing and potential actions to address these gaps, which form the basis of planned activities outlined in the SIP. The SIP was approved by Deputies from the various departments and agencies in November 2011.

Compliance with the Rule of Law

A fundamental precept of the SIP is that the Federal Government's actions must be consistent with the Constitution and in compliance with U.S. laws and regulations. Departments and agencies are responsible for identifying and complying with legal restrictions governing their activities and respective authorities. Compliance with the rule of law, particularly ensuring protection of First Amendment rights, is central to our National Strategy for Empowering Local Partners and the execution of the SIP.

Crosscutting and Supportive Activities

There are fundamental activities that are critical to our success and cut across the objectives of the SIP. These include: (1) whole-of-government coordination; (2) leveraging existing public safety, violence prevention, and community resilience programming; (3) coordination of domestic and international CVE efforts, consistent with legal limits; and (4) addressing technology and virtual space. In many instances, these crosscutting and supportive activities describe the ongoing activities of departments and agencies in fulfilling their broader missions. As they implement new initiatives and programs in support of the SIP, departments and agencies will ensure these enabling activities appropriately guide their efforts.

1. Whole-of-Government Coordination

Leveraging the wide range of tools, capabilities, and resources of the United States Government in a coordinated manner is essential for success. Traditional national security or law enforcement agencies such as DHS, DOJ, and the FBI will execute many of the programs and activities outlined in the SIP. However, as the National Strategy for Empowering Local Partners states, we must also use a broader set of good governance programs, "including those that promote immigrant integration and civic engagement, protect civil rights, and provide social services, which may also help prevent radicalization that leads to violence." To this end, agencies such as EDU and HHS, which have substantial expertise in engaging communities and delivering services, also play a role.

This does not mean the missions and priorities of these partners will change or that their efforts will become narrowly focused on national security. Their inclusion stems from our recognition that radicalization to violence depends on a variety of factors, which in some instances may be most effectively addressed by departments and agencies that historically have not been responsible for national security or law enforcement. These non-security partners, including specific components within DOJ and DHS, have an array of tools that can contribute to this effort by providing indirect but meaningful impact on CVE, including after school programs, networks of community-based organizations that provide assistance to new immigrants, and violence prevention programs. We will coordinate activities, where appropriate, to support the CVE effort while ensuring we do not change the core missions and functions of these departments and agencies.

2. Leveraging Existing Public Safety, Violence Prevention, and Resilience Programming

While preventing violent extremism is an issue of national importance, it is one of many safety and security challenges facing our Nation. As we enter an era of increased fiscal constraints, we must ensure our approach is tailored to take advantage of current programs and leverages existing resources. Our efforts therefore will be supported, where appropriate, by emphasizing opportunities to address CVE within available resources related to public safety, violence prevention, and building resilience.

3. Coordination of Domestic and International Efforts

While always ensuring compliance with applicable laws and regulations, we must ensure a high level of coordination between our domestic and international efforts to address violent extremism. Although both the National Strategy for Empowering Local Partners and the SIP specifically address preventing violent extremism in the United States, the delineation between domestic and international is becoming increasingly less rigid. Violent extremists operating abroad have direct access to Americans via the Internet, and overseas events have fueled violent extremist radicalization and recruitment in the United States. The converse is also true: events occurring in the United States have empowered the propaganda of violent extremists operating overseas. While making certain that they stay within their respective authorities, departments and agencies must ensure coordination between our domestic and international CVE efforts. Given its mandate to support both domestic and international planning, NCTC will help facilitate this part of the CVE effort so that our Homeland and overseas activities are appropriately synchronized, consistent with all applicable laws and regulations. While individual departments and agencies will regularly engage foreign partners, all international engagement will continue to be coordinated through State.

4. Addressing Technology and Virtual Space

The Internet, social networking, and other technology tools and innovations present both challenges and opportunities. The Internet has facilitated violent extremist recruitment and radicalization and, in some instances, attack planning, requiring that we consider programs and initiatives that are mindful of the online nature of the threat. At the same time, the Federal Government can leverage and support the use of new technologies to engage communities, build and mobilize networks against violent extremism, and undercut terrorist narratives. All of our activities should consider how technology impacts radicalization to violence and the ways we can use it to expand and improve our whole-of-government effort. As noted in sub-objective 3.3, we will develop a separate strategy focused on CVE online.

Roles and Responsibilities

The SIP assigns Leads and Partners in each of the Future Activities and Efforts listed under respective sub-objectives. Leads and Partners have primary responsibility for coordinating, integrating, and synchronizing activities to achieve SIP sub-objectives and the overall goal of the National Strategy for Empowering Local Partners.

Expectation of Leads and Partners are as follows:

Lead: A department or agency responsible for convening pertinent partners to identify, address, and report on steps that are being taken, or should be taken, to ensure activities are effectively executed. The Lead is accountable for, among other things:

- Fostering communication among Partners to ensure all parties understand how to complete the activity;
- Identifying, in collaboration with assigned Partners, the actions and resources needed to effectively execute the activity;
- Identifying issues that impede progress; and
- Informing all departments and agencies about the status of progress by the Lead and other sub-objective Partners, including impediments, modifications, or alterations to the plan for implementation.

Partner: A department or agency responsible for collaborating with a Lead and other Partners to accomplish an activity. Partner(s) are accountable for:

- Accomplishing actions under their department or agency's purview in a manner that contributes to the effective execution of an activity;
- Providing status reports and assessments of progress on actions pertinent to the activity; and
- Identifying resource needs that impede progress on their department or agency's activities.

Assessing Progress

It is important to recognize that the National Strategy for Empowering Local Partners represents the first time the United States Government has outlined an approach to address ideologically inspired violent extremism in the Homeland. While the objectives and sub-objectives listed in the SIP represent the collective wisdom and insight of the United States Government about what areas of action have the greatest potential to prevent violent extremism, we will learn more about our effectiveness as we assess our efforts over time, and we will adjust our activities accordingly.

Given the short history of our coordinated, whole-of-government approach to CVE, we will first develop key benchmarks to guide our initial assessment. Where possible, we will also work to develop indicators of impact to supplement these performance measures, which will tell us whether our activities are having the intended effects with respect to an objective or sub-objective. As we implement our activities, future evaluations will shift away from benchmark performance measures towards impact assessments. Departments and agencies will be responsible for assessing their specific activities in pursuit of SIP objectives, in coordination with an Assessment Working Group. We will develop a process for identifying gaps, areas of limited progress, resource needs, and any additional factors resulting from new information on the dynamics of radicalization to violence. Our progress will be evaluated and reported annually to the President.

Objectives, Sub-Objectives, and Activities

The SIP's objectives mirror the National Strategy for Empowering Local Partners' areas of priority action: (1) enhancing Federal engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals. Each of these is supported by sub-objectives, which constitute measurable lines of effort with which our specific programs and initiatives are aligned. A key purpose of the SIP is to describe the range of actions we are taking to improve or expand these efforts.

1. Enhancing Federal Engagement with and Support to Local Communities that May be Targeted by Violent Extremists

Communication and meaningful engagement with the American public is an essential part of the Federal Government's work, and it is critical for developing local partnerships to counter violent extremism. Just as we engage and raise awareness to prevent gang violence, sexual offenses, school shootings, and other acts of violence, so too must we ensure that our communities are empowered to recognize threats of violent extremism and understand the range of government and nongovernment resources that can help keep their families, friends, and neighbors safe. As noted in the National Strategy for Empowering Local Partners:

> Engagement is essential for supporting community-based efforts to prevent violent extremism because it allows government and communities to share information, concerns, and potential solutions. Our aims in engaging with communities to discuss violent extremism are to: (1) share sound, meaningful, and timely information about the threat of violent extremism with a wide range of community groups and organizations, particularly those involved in public safety issues; (2) respond to community concerns about government policies and actions; and (3) better understand how we can effectively support community-based solutions.

At the same time, we must ensure that our efforts to prevent violent extremism do not narrow our relationships with communities to any single issue, including national security. This necessitates continuing to engage on the full range of community interests and concerns, but it also requires, where feasible, that we incorporate communities that are being targeted by violent extremists into broader forums with other communities when addressing non-CVE issues. While we will engage with some communities specifically on CVE issues because of particular needs, care should be taken to avoid giving the false impression that engagement on non-security issues is taking place exclusively because of CVE concerns. To ensure transparency, our engagement with communities that are being targeted by violent extremists will follow two tracks:

- We will specifically engage these communities on the threat of violent extremism to raise awareness, build partnerships, and promote empowerment. This requires specific conversations and activities related to security issues.
- Where we engage on other topics, we will work to include them in broader forums with other communities when appropriate.

1.1 Improve the depth, breadth, and frequency of Federal Government engagement with and among communities on the wide range of issues they care about, including concerns about civil rights, counterterrorism security measures, international events, and foreign policy issues.

Violent extremist narratives espouse a rigid division between "us" and "them" that argues for exclusion from the broader society and a hostile relationship with government and other communities. Activities that reinforce our shared sense of belonging and productive interactions between government and the people undercut this narrative and emphasize through our actions that we are all part of the social fabric of America. As President Obama emphasized, when discussing Muslim Americans in the context of al-Qa'ida's attempts to divide us, "we don't differentiate between them and us. It's just us."

Current Activities and Efforts

Departments and agencies have been conducting engagement activities based on their unique mandates. To better synchronize this work, U.S. Attorneys, who historically have engaged with communities in their districts, have begun leading Federal engagement efforts. This includes our efforts to engage with communities to (1) discuss issues such as civil rights, counterterrorism security measures, international events, foreign policy, and other community concerns; (2) raise awareness about the threat of violent extremism; and (3) facilitate partnerships to prevent radicalization to violence. The types of communities involved in engagement differ depending on the locations. United States Attorneys, in consultation with local and Federal partners, are best positioned to make local determinations about which communities they should engage. Appointed by the President and confirmed by the Senate, U.S. Attorneys are the senior law enforcement and executive branch officials in their districts, and are therefore well-placed to help shape and drive community engagement in the field.

In December 2010, 32 U.S. Attorneys' Offices began expanding their engagement with communities to raise awareness about how the United States Government can protect all Americans from discrimination, hate crimes, and other threats; to listen to concerns; and to seek input about government policies and programs. In some instances, these efforts also included initiatives to educate the public about the threat of violent extremist recruitment, which is one of many components of a broader community outreach program.

- During this initial pilot, these U.S. Attorneys significantly expanded outreach and engagement on a range of issues of interest to communities; built new relationships where needed; and communicated the United States Government's approach to CVE.
- Departments and agencies, including State, the Treasury, EDU, HHS, and DHS provided information, speakers, and other resources for U.S. Attorneys' community engagement activities, frequently partnering with DOJ on specific programs and events.

A National Task Force, led by DOJ and DHS, was established in November 2010 to help coordinate community engagement at the national level. It includes all departments and agencies involved in relevant community engagement efforts and focuses on compiling local, national, and international best practices and disseminating these out to the field, especially to U.S. Attorneys' Offices. The Task Force is also responsible for connecting field-based Federal components to the full range of United States Government officials involved in community engagement to maximize partnerships,

coordination, and resource-sharing. The following are some examples of engagement efforts that are, or will be, coordinated with the Task Force:

- The DHS Office for Civil Rights and Civil Liberties (CRCL) this year doubled its outreach to communities and expanded its quarterly engagement roundtables to 14 cities throughout the country. During Fiscal Year 2011, CRCL also conducted 72 community engagement events, some of which included CVE-related topics.
- State engaged on U.S. foreign policy with a range of interested domestic communities. The Bureau of Near Eastern Affairs alone conducted 80 outreach events over the past year.
- DOJ has produced a number of brochures and other materials on civil rights protections and steps individuals can take to prevent or respond to discrimination, and has disseminated these to various communities, including those being targeted by violent extremists. DOJ has translated these materials into a number of languages, including Arabic, Somali, Urdu, Farsi, and Hindi.
- DOJ, in coordination with DHS, expanded the Building Communities of Trust (BCOT) Initiative, which focuses on developing relationships among local law enforcement departments, fusion centers, and the communities they serve to educate communities on: (1) the Nationwide Suspicious Activity Reporting Initiative (NSI); (2) how civil rights and liberties are protected; and (3) how to report incidents in order to help keep our communities safe. DOJ continues to support the BCOT Initiative.

Future Activities and Efforts

The primary focus for the next year will be: (1) expanding the scope of engagement; (2) building new partnerships between communities and local law enforcement, local government officials, and civil society; (3) incorporating communities that are being targeted by violent extremist radicalization into broader forums with other communities to engage on a range of non-security issues; and (4) increasing our engagement specifically on CVE. Additional activities going forward include the following:

- DOJ will incorporate more U.S. Attorneys' Offices as engagement leads in the field, building on the initial U.S. Attorney-led effort. (Lead: DOJ; Partners: All)
- The National Task Force will: (1) disseminate regular reports on best practices in community engagement to local government officials, law enforcement, U.S. Attorneys' Offices, and fusion centers; (2) work with departments and agencies to increase their support to U.S. Attorney-led engagement efforts in the field; and (3) closely coordinate Federal engagement efforts with communities targeted by violent extremist radicalization. (Leads: DOJ and DHS; Partners: All)
- In consultation with Federal and local partners, the National Task Force and the U.S. Attorneys' Offices will facilitate, where appropriate, the inclusion of communities that may be targeted by violent extremist radicalization into broader engagement forums and programs that involve other communities. (Leads: DOJ and DHS; Partners: All)
- U.S. Attorneys will coordinate closely with local government officials, law enforcement, communities, and civil society to enhance outreach events and initiatives. (Lead: DOJ; Partners: All)

- In Fiscal Year (FY) 2012, CRCL plans on expanding its quarterly community engagement roundtables to a total of 16. CRCL is also in the process of implementing a campus youth community engagement plan, through which it will engage with young adults on the topic of violent extremism. (Lead: DHS)
- Depending on local circumstances, and in consultation with the FBI and other agencies as appropriate, U.S. Attorneys will coordinate any expanded engagement specific to CVE with communities that may be targeted by violent extremist radicalization. (Lead: DOJ; Partners: DHS, NCTC, and FBI)
- An FBI CVE Coordination Office will be established and, as part of its activities, will coordinate with the National Task Force on CVE-specific education and awareness modules. These modules will be developed and implemented, in part, by leveraging some of the FBI's existing programs and initiatives. (Lead: FBI; Partners: DOJ and DHS)
- DHS will oversee an online portal to support engagement by government officials and law enforcement with communities targeted by violent extremist radicalization, which will be used to share relevant information and build a community of interest. The portal will be accessible to government officials and law enforcement involved in overseas and domestic CVE and community engagement efforts to share best practices. (Lead: DHS; Partners: State, and NCTC)
- DOJ will expand the efforts of the BCOT initiative to help facilitate trust between law enforcement and community leaders. This dialogue could include local issues, as well as CVE. (Lead: DOJ; Partner: DHS)
- The United States Government will build a digital engagement capacity in order to expand, deepen, and intensify our engagement efforts. Where possible, virtual engagement will build on real world engagement activities and programs. (Lead: DHS; Partners: All)

1.2 *Foster community-led partnerships and preventative programming to build resilience against violent extremist radicalization by expanding community based solutions; leveraging existing models of community problem-solving and public safety; enhancing Federal Government collaboration with local governments and law enforcement to improve community engagement and build stronger partnerships; and providing communities with information and training, access to resources and grants, and connections with the philanthropic and private sectors.*

The Federal Government can foster nuanced and locally rooted counter-radicalization programs and initiatives by serving as a facilitator, convener, and source of information to support local networks and partnerships at the grassroots level. Importantly, because the dynamics of radicalization to violence frequently vary from location to location, we recognize that a one-size-fits-all approach will be ineffective.

Current Activities and Efforts

The Federal Government has held a series of consultative meetings with communities, local government and law enforcement, civil society organizations, foundations, and the private sector to better understand how it can facilitate partnerships and collaboration. This leverages a key strength identified

in the National Strategy for Empowering Local Partners: "The Federal Government, with its connections to diverse networks across the country, has a unique ability to draw together the constellation of previously unconnected efforts and programs to form a more cohesive enterprise against violent extremism." Examples of this include the following:

- DHS Secretary Napolitano tasked her Homeland Security Advisory Council (HSAC) to develop recommendations on how the Department can best support law enforcement and communities in their efforts to counter violent extremism. An HSAC CVE Working Group convened multiple meetings with local law enforcement, local elected officials, community leaders (including faith-based leaders), and academics. The working group released its recommendations in August 2010, highlighting the importance of: (1) research and analysis of violent extremism; (2) engagement with communities and leveraging existing partnerships to develop information-driven, community-based solutions to violent extremism and violent crime; and (3) community oriented policing practices that focus on building partnerships between law enforcement and communities.
- DHS and NCTC began raising awareness about violent extremism among private sector actors and foundations and connected them with community civic activists interested in developing programs to counter violent extremism. DHS is now working with a foundation to pilot resiliency workshops across the country that address all hazards, including violent extremism.

We also began exploring how to incorporate CVE as an element of programs that address broader public safety, violence prevention, and resilience issues. This has the advantage of leveraging preexisting initiatives and incorporates CVE in frameworks (such as safeguarding children) used by potential local partners who may otherwise not know how they fit into such efforts. For example, although many teachers, healthcare workers, and social service providers may not view themselves as potentially contributing to CVE efforts, they do recognize their responsibilities in preventing violence in general. CVE can be understood as a small component of this broader violence prevention effort. Departments and agencies will review existing public safety, violence prevention, and resilience programs to identify ones that can be expanded to include CVE as one among a number of potential lines of effort.

- As an example, the Federal Government helped support a community-led initiative to incorporate CVE into a broader program about Internet safety. The program addressed protecting children from online exploitation, building community resilience, and protecting youth from Internet radicalization to violence.

Future Activities and Efforts

Planned activities to expand support to local partners include the following:

- The Federal Government will help broker agreements on partnerships to counter violent extremism between communities and local government and law enforcement to help institutionalize this locally focused approach. (Lead: DHS)
- DHS and DOJ will work to increase support for local, community-led programs and initiatives to counter violent extremism, predominantly by identifying opportunities within existing appropriations for incorporating CVE as an eligible area of work for public safety, violence prevention, and community resilience grants. (Leads: DHS and DOJ)

- DHS is working to increase funding available to integrate CVE into existing community-oriented policing efforts through FY12 grants. (Lead: DHS)
- DHS is establishing an HSAC Faith-Based Community Information Sharing Working Group to determine how the Department can: (1) better share information with faith communities; and (2) support the development of faith-based community information sharing networks. (Lead: DHS)
- DHS is developing its Hometown Security webpage to include resources such as training guidance, workshop reports, and information on CVE for both the general public and law enforcement. (Lead: DHS)
- The Treasury will expand its community outreach regarding terrorism financing issues. (Lead: Treasury; Partners: State, DOJ, DHS, FBI, and the U.S. Agency for International Development)[3]
- Depending on local circumstances and in consultation with the FBI, U.S. Attorneys will coordinate, as appropriate, any efforts to expand connections and partnerships at the local level for CVE, supported by the National Task Force where needed. (Lead: DOJ; Partners: All)
- Departments and agencies will expand engagement with the business community by educating companies about the threat of violent extremism and by connecting them to community civic activists focused on developing CVE programs and initiatives. (Lead: DHS; Partner: NCTC)

2. Building Government and Law Enforcement Expertise for Preventing Violent Extremism

It is critical that the Federal Government and its local government and law enforcement partners understand what the threat of violent extremism is, and what it is not. This helps ensure that we focus our resources where they are most effective and that we understand how we can best empower and partner with communities. Building expertise necessitates continued research about the dynamics of radicalization to violence and what has worked to prevent violent extremism; sharing this information as widely as possible; and then leveraging it to train government officials and law enforcement.

2.1 Improve our understanding of violent extremism through increased research, analysis, and partnerships with foreign governments, academia, and nongovernmental organizations.

The Federal Government has built a robust analytic program to understand violent extremism that includes analysis; research conducted by academia, think tanks, and industry; and exchanges with international allies to identify best practices. While we have increased our understanding of how individuals are radicalized to violence, we must continue to identify gaps, monitor changes in the dynamics of violent extremism, and remain vigilant by challenging our assumptions and continuing our research and analysis.

Current Activities and Efforts

The United States Government's research capacity on this issue has greatly expanded. DHS and NCTC both have analytic groups exclusively focused on violent extremist radicalization; the Interagency Intelligence Subcommittee on Radicalization helps coordinate and improve CVE intelligence analysis; and we work with foreign governments, academia, and nongovernmental organizations to inform and

[3] The U.S. Agency for International Development's role will be limited to sharing relevant information.

supplement our analysis and understanding. In addition to a large volume of intelligence products on CVE, examples of activities include:

- DHS Science & Technology (S&T) sponsored research on violent extremism in the United States, which it has shared with DHS components and other departments and agencies. Over 20 reports have been produced since 2009 and 5 more will be produced by the end of 2011. DHS is also developing an integrated open source database to help inform CVE programs.
- DHS's Office of Intelligence and Analysis (I&A) collaborated with the FBI, the Bureau of Prisons (BOP), and NCTC to assess the capacity of state correctional institutions to detect and share information regarding individuals who demonstrate behaviors associated with violent extremism while in the correctional system.
- The National Intelligence Council, DHS, FBI, and NCTC briefed fusion centers and law enforcement around the country on violent extremism.
- DHS, in partnership with the FBI and NCTC, developed case studies on preoperational indicators and known threats for State and local law enforcement and affected communities.
- The United States Government held regular exchanges of best practices with Australia, Canada, Denmark, Germany, the European Union, the Netherlands, the United Kingdom, and other partners to gain comparative insights about what might be effective in the Homeland.
- DHS expanded cooperation between the United States and Canada on CVE research and lessons learned.
- The United States Government participates in the Global Counterterrorism Forum's CVE Working Group.
- As directed in the Fort Hood Follow-on Review, DOD established the Force Protection Senior Steering Group. Among the Steering Group's duties is the coordination of non-traditional partners' activities within DOD (e.g., counterintelligence and behavioral health) to better understand how to identify and prevent all forms of violent extremism—not limited to al-Qa'ida-inspired extremism—within the military, including the potential use of DOD's extensive network of programs designed to support individuals who are potentially at risk of committing acts of violence against themselves, their families, or co-workers.

Future Activities and Efforts

Although we have a better understanding of the threat, there are gaps that need to be addressed through additional research and analysis. In this regard, we will:

- Expand analysis in five priority areas (Leads: DHS, FBI, NCTC, and State):
    1. The role of the Internet in radicalization to violence and how virtual space can be leveraged to counter violent extremism.
    2. Single-actor terrorism (so called "lone wolves"), including lessons learned from similar phenomena such as a school shooters.
    3. Disengagement from terrorism and violent extremism.

4. Non-al-Qa'ida related radicalization to violence and anticipated future violent extremist threats.
5. Preoperational indicators and analysis of known case studies of extremist violence in the United States.

- Continue DHS S&T's support for research on countering the threat of extremist violence. (Lead: DHS)
- Continue DHS collaboration with the FBI, the BOP, and NCTC to: (1) improve awareness of the risk of violent extremism in correctional systems; (2) enhance screening of new inmates to detect individuals associated with violent extremist organizations; (3) improve detection of recruitment efforts within the correctional environment; and (4) increase information sharing, as appropriate, with Federal, State, and local law enforcement about inmates who may have adopted violent extremist beliefs and are being released. (Lead: DHS; Partners: DOJ, FBI, and NCTC)
- Complete the creation of the FBI CVE Coordination Office to help assess and leverage existing Bureau efforts to better understand and counter violent extremism. (Lead: FBI)
- Build lines of research specifically to support non-security Federal partners. (Leads: DHS and NCTC; Partners: EDU and HHS)

2.2 Increase Federal Government information sharing with State, local, and tribal governments and law enforcement on terrorist recruitment and radicalization.

As we enhance our partnerships with State, local, and tribal governments and law enforcement to counter violent extremism, it is essential that we share our expertise and insights about the dynamics of radicalization to violence and what has worked to prevent it. This, in turn, will help our partners identify potential areas of collaboration with communities and other local actors.

Current Activities and Efforts

Examples include:

- Based on direction from the Office of the Director of National Intelligence (DNI), DHS led an effort to improve the analysis of homegrown violent extremism, including analytic tools to share with State, local, and tribal partners. DHS briefed representatives of 47 states on the project.
- DHS generated case studies of known and suspected terrorists and assessments of radicalization to violence, based on recent arrests, to share with local partners.
- FBI disseminated information to public safety partners, including information about radicalization to violence.
- DHS, NCTC, and FBI briefed and disseminated information on how individuals are radicalized to violence to law enforcement, fusion centers, and local government officials, including the Major Cities Chiefs, representatives from 47 states, Mayors' Offices, and State Homeland Security Advisors.

- In partnership with NCTC, DOJ, DNI, and FBI, DHS led the first National CVE Workshop in August 2011, which brought together intelligence commanders from major metropolitan areas and fusion center directors to increase their understanding of CVE.

Future Activities and Efforts

More work needs to be done to ensure our State, local, and tribal partners have the information they need to counter violent extremism. Classification remains an obstacle to broader sharing with these partners, but we can better ensure that analytic production is tailored to the needs of practitioners in the field. Major work over the next year will focus on creating more analytic products on CVE that directly support local law enforcement and government. Planned actions include:

- Development of an analytic team focused on supporting local government and law enforcement CVE practitioners and increased production of analysis at appropriate classification levels. (Lead: DHS; Partners: FBI and NCTC)
- Development of practitioner-friendly summaries of current research and literature reviews about the motivations and behaviors associated with single-actor terrorism and disengagement from violent extremism. (Lead: DHS)
- Review of information-sharing protocols to identify ways of increasing dissemination of products to State, local, and tribal authorities. (Leads: DHS, DOJ, FBI, and NCTC)
- Expansion of briefings and information sharing about violent extremism with State and local law enforcement and government. (Lead: DHS, FBI, and NCTC)

2.3 *Improve the development and use of standardized training with rigorous curricula based on the latest research, which conveys information about violent extremism; improves cultural competency; and imparts best practices and lessons learned for effective community engagement and partnerships.*

The Federal Government has expanded and improved training related to CVE over the past year, but challenges remain. In particular, there is a need for a review process and standards for training specific to CVE, which was underscored by a small number of instances of Federally sponsored or funded CVE-related and counterterrorism training that used offensive and inaccurate information, which was inconsistent with our values and core principles. As our National Strategy to Empower Local Partners highlights, "Misinformation about the threat and dynamics of radicalization to violence can harm our security by sending local stakeholders in the wrong direction and unnecessarily creating tensions with potential community partners." Therefore, improving Federal Government-approved training practices and processes related to CVE is a top priority of this plan.

Current Activities and Efforts

In November 2010, the IPC tasked DHS to form an Interagency Working Group on Training to catalogue and recommend improvements for CVE-related training across government. The Working Group brought together individuals responsible for CVE training and substantive specialists from civil rights and civil liberties offices, Federal law enforcement, and the analytic community. This is part of our overall

emphasis on improving the quality and quantity of CVE-related training. Notable accomplishments in our efforts to improve training include:

- Between October 2010 and October 2011, DHS CRCL trained nearly 2,700 law enforcement officials on CVE and cultural awareness at 46 separate events. The training served as the basis for best practices recommended by the Interagency Working Group on Training.
- Based on input from participating agencies, DHS issued CVE training guidance and best practices in October 2011 for Federal, State, local, and tribal government officials charged with organizing training related to CVE, cultural awareness, and counterterrorism.
- The Federal Emergency Management Agency (FEMA) in October 2011 issued an Information Bulletin on CVE Training, which includes DHS's training guidance and best practices, as well as guidance for State, local, and tribal entities that regularly leverage FEMA grants to fund CVE-related trainings. DHS sent the best practices paper and the FEMA guidance to all DHS grantees, State and local governments, State and local law enforcement, relevant community stakeholders, and interagency partners.
- DHS provided a full-day of training, which included training on cultural competency, civil rights, and civil liberties to Federal, State, local, and tribal partners at 12 fusion centers in the past year and over 30 fusion centers since 2008. These trainings were coupled with 3- to 4-hour CVE training sessions for State and local law enforcement operating in the same state. Additionally, DHS provided "train the trainer" sessions for staff from nearly all fusion centers nationwide.
- DHS, working closely with other departments and agencies, local law enforcement, academics, and curriculum development experts, developed guidelines for a CVE curriculum that focuses on information-driven community-oriented policing practices and how to leverage existing community partnerships to counter violent extremism and violent crime. These guidelines were reviewed and validated in February 2011 at a "proof-of-concept" session at the Federal Law Enforcement Training Center (FLETC), which was attended by State, local, and tribal law enforcement executives and frontline officers from rural and major city jurisdictions.
- State, working closely with NCTC and DHS, piloted specialized CVE training for United States Government officials working on CVE in the United States and abroad through its Foreign Service Institute in May 2011. Participation by domestic and international practitioners provided opportunities for exchanging best practices, enhanced the coordination of our Homeland and overseas efforts, and encouraged interagency partnerships.

Future Activities and Efforts

A review process by the Interagency Working Group on Training, as well as internal assessments by departments and agencies, indentified two key challenges, which we will address over the next year:

- Many departments and agencies lack a review process for training materials and outside speakers on CVE, which led to a small number of cases of training that violated internal principles as well as core tenets of the National Strategy to Empower Local Partners.

- There has been a lack of guidance and standards for training related to CVE, which left field offices, in particular, vulnerable to bad training. Without guidance or standards, it has been difficult to enforce accountability.

We have prioritized addressing these two shortcomings by doing the following:

- Departments and agencies are taking steps to identify training materials that may not meet internal standards and to improve processes for creating and reviewing such materials. Some departments are consulting with outside experts with established reputations to evaluate the content and training review process. Guidance on CVE-related training is being developed and will be issued, both across the organizations and to field components. Some departments may issue this as part of broader training guidance. (Lead: All)
- DHS, via FLETC, is in the process of developing a CVE curriculum to be integrated into existing training programs for Federal law enforcement. The curriculum will give Federal law enforcement a better understanding of CVE and how to more effectively leverage existing local partnerships. (Lead: DHS)
- DHS is in the process of establishing an internal committee to review all directly funded and issued DHS training on cultural competency, engagement, CVE, and counterterrorism. The committee will be responsible for reviewing any new content, evaluating experts, and establishing quality control. FEMA will incorporate the recently released Informational Bulletin and training guidance into FY12 grant guidance and will also leverage existing mechanisms to hold grantees and sub-grantees accountable. (Lead: DHS)

In addition to addressing the quality issue, we will work to expand the quantity of training.

- DHS, in partnership with the Los Angeles Police Department and the National Consortium for Advanced Policing, is developing a CVE curriculum that includes a 16-hour continuing education module for executive and frontline officers, as well as a 30-minute module that will be introduced at police academies. Both will be certified by the Police Officers Standards and Training Council. In October 2011 the Major Cities Chiefs Association passed a motion to adopt and implement the DHS CVE curriculum, which will be piloted with State and local law enforcement in San Diego by the end of 2011. By 2013, DHS seeks to: (1) implement the curriculum across the country on a regional basis; (2) develop a national network of trainers and subject matter experts who can administer the training and keep it current; and (3) build an online component for the curriculum. (Lead: DHS; Partners: DOJ and NCTC)
- DHS, via FLETC, will update current Federal training programs to integrate the CVE curriculum for Federal law enforcement in the coming year. (Lead: DHS)
- DHS is working with European law enforcement partners to share best practices and case studies to improve training, community policing, and operational information sharing. (Lead: DHS)
- DHS CRCL is expanding and institutionalizing its CVE and cultural competence training curricula to further enhance the material and its effectiveness. (Lead: DHS)

- The Interagency Working Group on Training will facilitate a "train the trainer program" to increase the reach of CVE training. (Leads: DHS and NCTC; Partners: DOJ, EDU, HHS, and FBI)
- The Interagency Working Group on Training will facilitate the development of an online training program that provides professional development credit for a broad range of professions, particularly those involved with public safety, violence prevention, and resilience. This will help build a basic understanding of CVE among a broad cross-section of stakeholders who have related mandates. (Leads: DHS and NCTC; Partners: DOJ, FBI, EDU, and HHS)
- The Interagency Working Group on Training will collaborate with non-security partners, such as EDU, to build CVE training modules that can be incorporated, as appropriate, into existing programs related to public safety, violence prevention, and resilience. These modules will be crafted in a way that is relevant to the specific audiences and their missions. Only trainers who have undergone CVE-specific training will deliver training programs that include CVE modules. (Lead: DHS; Partners: DOJ, EDU, HHS, FBI, and NCTC)
- DOD's training programs and curricula will be informed by the work of the Interagency Working Group on Training, as appropriate. Additionally, DOD is conducting a review of CVE-related curricula and will make revisions and adjustments as necessary. (Lead: DOD; Partner DHS)

3. Countering violent extremist propaganda while promoting our ideals

As the National Counterterrorism Strategy emphasizes, "[t]he United States was founded upon a belief in a core set of values that is written into our founding documents and woven into the very fabric of our society. Where terrorists offer injustice, disorder, and destruction the United States must stand for freedom, fairness, equality, dignity, hope, and opportunity. The power and appeal of our values enables the United States to build a broad coalition to act collectively against the common threat posed by terrorists, further delegitimizing, isolating, and weakening our adversaries."

Countering the ideologies and narratives that legitimize violence is central to our effort, but it also is the most challenging area of work, requiring careful consideration of a number of legal issues, especially those related to the First Amendment. In many instances, it will be more effective to empower communities to develop credible alternatives that challenge violent extremist narratives rather than having the Federal Government attempt to do so.

Our efforts include not only challenging justifications for violence, but affirming American ideals of inclusiveness and opportunity as well. Violent extremist narratives feed on disenchantment and the sense of exclusion. Our efforts therefore must include positive affirmation of our unity as a country. To some extent, this is addressed through our engagement activities, particularly where they address challenges facing all communities and not just those targeted by violent extremist radicalization. But there are also situations where we will need to more directly challenge violent extremist narratives.

3.1 Increase the capacity of communities to directly challenge violent extremist ideologies and narratives.

While the government cannot always directly contest violent extremist ideas, it can support capacity building within communities to take on this role. Whereas sub-objective 1.2 emphasizes preventative

measures and a defensive posture to build capacity for enhancing community resilience, sub-objective 3.1 focuses on increasing the ability of communities to push back against violent extremist propaganda.

Current Activities and Efforts

Most of our work in this area to date has focused on connecting community activists to potential civil society and private sector partners to focus specifically on undermining violent extremist narratives. Over the past year, we have taken the following steps:

- NCTC in 2010 developed a Community Awareness Briefing (CAB) to inform members of the public about efforts by al-Qa'ida and its adherents and affiliates to recruit Americans. The CAB highlights recruiting videos and examples of violent extremist propaganda, while underscoring the fact that these materials are often easily available on the Internet. Most importantly, the CAB aims to facilitate a discussion about what government and communities can do, together and independently, to counter the threat of violent extremist narratives. NCTC continues to deliver the presentation at forums composed of community leaders, educators, and parents in cities across the United States. In March 2011, NCTC held a workshop for local, State, and field-based Federal officials on how the CAB could be used in engagement efforts, when it makes sense and is appropriate.
- NCTC connected civic activists with technology experts, resulting in a training seminar on how to maximize the use of technology to counter violent extremism online.
- State sponsored speaker series and exchanges between international CVE practitioners and American communities targeted by violent extremist recruiters to better understand effective models for countering violent extremist narratives.

Future Activities and Efforts

This is a nascent area of effort and therefore will necessitate greater focus over the next year. Our planned actions include:

- Expanding efforts to raise community awareness about the threat of radicalization to violence, building from the experience of the CAB, and adapting those materials for different audiences where appropriate. (Leads: DOJ, DHS, FBI, and NCTC)
- Learning from former violent extremists, specifically those who can speak credibly to counter violent narratives, provide insights to government, and potentially catalyze activities to directly challenge violent extremist narratives. (Lead: DHS; Partner: NCTC)
- Providing grants to counter violent extremist narratives and ideologies, within authorities and relevant legal parameters, by reprioritizing or increasing the flexibility of existing funding. (Lead: DHS)
- Brokering connections between private sector actors, civil society, and communities interested in countering violent extremist narratives. (Lead: DHS; Partner: NCTC)
- Promoting international exchange programs to build expertise for countering violent extremist narratives. (Lead: State; Partners: DDJ, DHS, FBI, and NCTC)

- Increasing technical training to empower communities to counter violent extremists online, including the development of training for bloggers. (Lead: DHS; Partners: State, NCTC, and FBI)

3.2 Improve and increase our communication to the American public about the threat posed by violent extremist groups, myths and misperceptions about violent extremist radicalization, and what we are doing to counter the threat.

It is important that we communicate to the American public the realities of what the threat is, and what it is not. Misconceptions about the threat and statements and actions that cast suspicion on entire communities based on the actions of a few distract attention from the real threat and can undermine our ability to build partnerships. An informed citizenry enhances our national security.

Current Activities and Efforts

In 2011, the Federal Government focused on developing its approach to domestic CVE and communicating this to the American public. This involved briefings to Congress, public addresses, and media interviews. We will continue these activities.

Future Activities and Efforts

In 2012, we will work to expand our efforts to raise awareness in the general public about radicalization to violence in the United States and the tools to prevent it by:

- Providing regular briefings to Congress, think tanks, and members of the media. (Lead: DHS; Partners: DOJ, FBI, and NCTC)
- Creating programs to directly engage the public on the issue. (Lead: All)
- Building a public website on community resilience and CVE. (Lead: DHS)

3.3 Build a strategy ta leverage new technologies and address online violent extremist radicalization

The Internet has become an increasingly potent element in radicalization to violence, enabling violent extremists abroad to directly communicate to target audiences in the United States. This direct communication allows violent extremists to bypass parents and community leaders. The SIP specifically addresses the online arena in several sub-objectives, but because of the importance of the digital environment, we will develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience that considers: (1) the latest assessment of the role of the Internet; (2) the absence of clear national boundaries in online space and the relationship between international and domestic radicalization to violence; (3) relevant legal issues; and (4) the differing authorities and capabilities of departments and agencies.

Conclusion

Protecting our Nation's communities from violent extremist recruitment and radicalization is a top national security priority. It is an effort that requires creativity, diligence, and commitment to our fundamental rights and principles. In his cover letter to the National Strategy for Empowering Local Partners, President Obama wrote:

> Sadly, the threat of violent extremism in America is nothing new. Throughout our history, misguided groups—including international and domestic terrorist organizations, neo-Nazis and anti-Semitic hate groups—have engaged in horrific violence to kill our citizens and threaten our way of life. Most recently, al-Qa'ida and its affiliates have attempted to recruit and radicalize people to terrorism here in the United States, as we have seen in several plots and attacks, including the deadly attack 2 years ago on our service members at Fort Hood. As a government, we are working to prevent all types of extremism that leads to violence, regardless of who inspires it.
>
> —President Barack Obama, August 3, 2011

A complex issue like violent extremist radicalization and recruitment requires a nuanced path to guide a whole-of-government approach. The SIP outlines this path and facilitates a division of labor by assigning responsibilities between Federal Government departments, agencies, and components focused on law enforcement and national security and those whose efforts support, but do not directly lie within, these areas.

Faith-Based Homeland Security and Communications Advisory Committee (FBAC) Meeting

March 9, 2012, NAC, BLDG 1, Large Conference Room (44)

AGENDA:

8:30 a.m.	Welcome ((b)(6)
8:45 a.m.	Case Studies on I&A work with Faith-based Partners (b)(6)
9:25 a.m.	Case Studies on State/Major Urban Area FCs work with Faith-based Partners (b)(6)
10:00 a.m.	Building Trust with our Faith-based Partners (b)(6)
10:45 a.m.	State and Local Law Enforcement Panel Information Sharing with FBAC (b)(6)
12:15pm	**Working Lunch – DHS CVE Community Partnership Approach and SAR** (b)(6) **Principal Deputy Counter Terrorism Coordinator and Senior Advisor to the Secretary** **Overview of "If You See Something, Say Something™"** (b)(6))
1:15 pm	BREAK
1:30 pm	DHS Working with Faith-based Organizations ((b)(6) (b)(6)
2:30 pm	DHS Deepening the Partnership with FBOs ((b)(6))
3:20 pm	Next Steps/Closing Remarks (Co-Chairs and Co-Vice Chairs)

OBJECTIVE:

To provide an overview of DHS' information sharing programs with faith-based communities and to provide guidance to develop recommendations for the FBAC's final report to the HSAC by May, 2012.

TALKING POINTS:

- Thank everyone for participating in this important initiative. Mention the importance of this Faith Based Homeland Security and Communications Advisory Committee to the Secretary and to the Department's overall CVE efforts.
- Reiterate to participants that their feedback and the recommendations they provide to the Secretary on how the Department can better work with faith based communities are critical.
- Describe how DHS has already implemented a number of the HSAC CVE Working Group recommendations and that DHS will take the recommendations from this group just as seriously and work to implement them.
- Reiterate that the case studies that have been presented today illustrate the crucial need for partnerships between law enforcement and faith based communities.

OVERALL BACKGROUND:

- This meeting and tasking originated from a meeting with Faith-Based leaders in 2010; at that time it was suggested that the HSAC CVE Working Group develop recommendations before a formal HSAC Faith-Based Advisory Committee was created.
- YOU have the opportunity to set the stage and provide concrete guidance to members as they develop their recommendations to the Secretary.

- YOU working lunch presentation will be following discussions on case studies that are being provided by:
  - (b)(6) from Dearborn regarding the Florida pastor incident
  - (b)(6) from Minneapolis regarding her work with the Somali community
  - (b)(6) from LA Sheriff's on the work they have done in regards to community engagement
- The case studies illustrate the crucial need for partnerships between law enforcement and communities. This point will need to be stressed and illustrated to members that partnerships are beneficial overall.
- (b)(6) will be at this meeting and are all former HSAC CVE Working Group members.

"If You See Something, Say Something™" BACKGROUND INFORMATION:
The Department is tying the launch of "If You See Something, Say Something ™" to those locations that are part of the Nationwide Suspicious Activity Reporting Initiative (NSI), which provides training to ensure that potential SARs are handled the appropriate way, ensures that privacy and civil rights & civil liberties protections are in place and that if there is a credible SAR, there is a mechanism in place to pass that information along to the appropriate federal partners for further investigation.

In June 2011, at a meeting in the Roosevelt Room at the White House, Secretary Napolitano met with leaders from the Jewish community, Jewish Federation of North America and SCN and agreed to partner on the "If You See Something, Say Something ™" campaign. The Department has created materials for the Jewish community to be used at synagogues, community centers, schools, federations, facilities and buildings. The campaign has been rolled out to the Jewish community in New York, New Jersey and will be tailored and expanded for additional locations in the coming weeks and months.

IMPORTANT POINTS:

- DHS ties all launches and partnerships of "If You See Something, Say Something ™" to or in places that are part of the NSI.
- All materials are designed and customized by DHS to ensure that they work for the entity that we're partnering with. (Sara will pass materials for the Jewish community to the group)
- We stress that it's important for people to pay attention to suspicious behaviors and activities and to not focus on a person's race, religion, etc.
- Upon request, we translate materials into other languages.
- We are eager to work with all religious communities on this initiative and look forward to doing so in a way that meets their needs/interests.

POSSIBLE QUESTIONS:

- What are the campaign's protections against racial or other identity-based profiling? What are the privacy protections?
- What mechanisms are in place to ensure compliance with civil rights protections as well as grievance procedures for individuals who have been discriminated against?

SIP BACKGROUND

- On December 8, 2011, after 5 months of planning and consultation with interagency partners, the White House released the Strategic Implementation Plan (SIP) for the Administration's CVE Strategy.
- The SIP lists the current and future actions the USG will take in support of a locally-focused, community-based approach, in three broad areas:
  - **Enhancing Engagement with and support to local communities:** Our aims in engaging with communities to discuss violent extremism are to (1) share sound, meaningful, and timely information about the threat of radicalization to violence with a wide range of groups and organizations; (2) respond to concerns about government policies and actions; and (3) better understand how we can effectively support community-based solutions.
  - **Building Government and Law Enforcement Expertise:** We are building robust training programs to ensure that communities, government, and law enforcement receive accurate, intelligence-based information about the dynamics of violent extremism. Misinformation about the threat and poor training harms our security by sending stakeholders in the wrong direction and creating tensions with communities.
  - **Countering Violent Extremist Propaganda while Promoting our Ideals:** We will aggressively counter violent extremist ideologies – including on the Internet – by educating and empowering communities and promoting our ideals. In the case of our current priority, we will, through our words and deeds, rebut al-Qa'ida's lie that the United States is somehow at war with Islam.
- The SIP Approach underscores the strength of community-based problem solving, local partnerships, and community-oriented policing. We are building our efforts from existing structures, while creating capacity to fill gaps as we implement programs.

IF ASKED

- **How is DHS working to implement the priorities in the SIP?**
  - DHS' Internal CVE Working Group meets weekly to ensure the priorities of the SIP are being implemented and is tracking the progress of each individual priority. DHS, NCTC, DOJ, and the FBI have committed to forming a small working group to meet on a bi-weekly basis to ensure the priorities in the SIP are implemented in a timely manner. The interagency also coordinated the development of the SIP through the multiple Deputies Breakfast meetings, and will continue to advance the priorities in the SIP through these meetings.
- **How is DHS ensuring that its training and curriculum development is coordinated with the interagency and meets the mutual standards agreed upon by the interagency?**
  - DHS created a CVE Curriculum Working Group on September 17, 2010, chaired by LAPD Deputy Chief Michael Downing, as a result of the HSAC recommendations that were issued in August, 2010, and this Curriculum Working Group was comprised of representatives from the federal government and state and local law enforcement entities. This working group met multiple times to discuss best practices for community policing and ultimately created a new curriculum guidance based on mutually agreed upon standards and definitions.

  - DHS is currently establishing an internal training review process that will look at all DHS provided and funded CVE trainings; it will ensure that all DHS trainings are in line with Department and Administration approach on CVE.
  - FEMA issued training guidance with an informational bulletin to all grantees, state and local partners, and law enforcement outlining how training and trainers should accurate, intelligence driven, legally following civil rights and civil liberties protections, and operationally sound.
  - The guidance is based off the work of the Interagency Law Enforcement Training Working Group that is lead by DHS and continues to meet.
- **What is the status and anticipated timeline for the development of CVE curriculum?**
  - DHS is currently in the process of developing a comprehensive CVE curriculum for federal, state, local, and tribal law enforcement focused on a community oriented policing approach to combat violent crime and counter violent extremism.
  - DHS along with state and local partners (LAPD/National Consortium for Advance Policing) is developing a CVE curriculum that will be introduced into law enforcement academies as well as a 16 hour continuing education curriculum that will be focused on executive and front line officers. The curriculum will be POST certified and rolled out regionally with a network of approved local CVE trainers.
    - The Curriculum was piloted successfully in San Diego on January 25-27th and included front-line and executive officers from the San Diego area.
  - The Major Cities Chief Association recently passed a motion to adopt and implement the curriculum; San Diego PD will pilot the curriculum.
  - FLETC finished the development of a CVE curriculum that will be integrated into existing training programs for federal law enforcement that will focus on cultural awareness, engagement practices, and how best to work with local law enforcement and communities to keep local partnerships intact. FLETC piloted an overview of the curriculum on February, 16, 2012 in Glynco, GA.

PARTICIPANTS:

Staff Responsible for Briefing Memo: (b)(6) Counterterrorism Working Group and (b)(6) OPA

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

NATIONAL SECURITY STAFF

Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States

> As a government, we are working to prevent all types of extremism that leads to violence, regardless of who inspires it. At the same time, countering al-Qa'ida's violent ideology is one part of our comprehensive strategy to defeat al-Qa'ida. Over the past 2½ years, more key al-Qa'ida leaders—including Usama bin Laden—have been eliminated in rapid succession than at any time since the September 11 attacks. We have strengthened homeland security and improved information sharing. Thanks to coordinated intelligence and law enforcement, numerous terrorist plots have been thwarted, saving many American lives.
>
> —*President Barack Obama, August 2011*

Law enforcement and government officials for decades have understood the critical importance of building relationships, based on trust, with the communities they serve. Partnerships are vital to address a range of challenges and must have as their foundation a genuine commitment on the part of law enforcement and government to address community needs and concerns, including protecting rights and public safety. In our efforts to counter violent extremism, we will rely on existing partnerships that communities have forged with Federal, State, and local government agencies. This reliance, however, must not change the nature or purpose of existing relationships. In many instances, our partnerships and related activities were not created for national security purposes but nonetheless have an indirect impact on countering violent extremism (CVE).

At the same time, this Strategic Implementation Plan (SIP) also includes activities, some of them relatively new, that are designed specifically to counter violent extremism. Where this is the case, we have made it clear. It is important that both types of activities be supported and coordinated appropriately at the local level.

Background

The President in August 2011 signed the *National Strategy for Empowering Local Partners to Prevent Violent Extremism in the United States* (National Strategy for Empowering Local Partners), which outlines our community-based approach and the Federal Government's role in empowering local stakeholders to build resilience against violent extremism.[1] It recognizes that, as the National Security Strategy from May 2010 highlights, "our best defenses against this threat are well informed and equipped families, local communities, and institutions." To support our overarching goal of preventing violent extremists and their supporters from inspiring, radicalizing, financing, or recruiting individuals or groups in the

[1] The National Strategy for Empowering Local Partners defines violent extremists as "individuals who support or commit ideologically motivated violence to further political goals."

United States to commit acts of violence, the Federal Government is focused on three core areas of activity: (1) enhancing engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals.

The SIP details how we are implementing the National Strategy for Empowering Local Partners. It explains our core objectives and sub-objectives; describes how activities by departments and agencies are aligned with these; lists planned activities that address gaps and expand efforts; and assigns Federal Government leads and partners for various actions. The SIP provides a blueprint for how we will build community resilience against violent extremism.[2] It does not address our overseas CVE efforts, other than ensuring we coordinate domestic and international activities.

Although the SIP will be applied to prevent all forms of violent extremism, we will prioritize preventing violent extremism and terrorism that is inspired by al-Qa'ida and its affiliates and adherents, which the 2010 National Security Strategy, the 2011 National Strategy for Counterterrorism, and the National Strategy for Empowering Local Partners identify as the preeminent security threats to our country. This is, however, a matter of emphasis and prioritization, and does not entail ignoring other forms of violent extremism. As the July 2011 terrorist attack in Norway underscored, free societies face threats from a range of violent extremists.

As the activities described in the SIP are executed, there will be major and long-lasting impacts:

- There will be platforms throughout the country for including communities that may be targeted by violent extremists for recruitment and radicalization into ongoing Federal, State, and local engagement efforts;
- The Federal Government will support that engagement through a task force of senior officials from across the government;
- Community-led efforts to build resilience to violent extremism will be supported;
- Analysis will increase in depth and relevance, and will be shared with those assessed to need it, including Governor-appointed Homeland Security Advisors, Major Cities Chiefs, Mayors' Offices, and local partners;
- Training for Federal, State, tribal, and local government and law enforcement officials on community resilience, CVE, and cultural competence will improve, and that training will meet rigorous professional standards; and
- Local partners, including government officials and community leaders, will better understand the threat of violent extremism and how they can work together to prevent it.

[2] The concept of "resilience" has applied to a range of areas such as emergency preparedness and critical infrastructure protection (e.g., the ability of financial markets, power suppliers, and telecommunications companies to withstand an attack or disaster and resume operations rapidly.) The National Security Strategy emphasized the importance of including individuals and communities in our approach to enhancing resilience. Both the National Strategy for Empowering Local Partners and the 2011 National Strategy for Counterterrorism expanded this concept to CVE, the latter explicitly stating, "We are working to bring to bear many of these capabilities to build resilience within our communities here at home against al-Qa'ida inspired radicalization, recruitment, and mobilization to violence."

The SIP outlines ongoing, as well as planned, activities to counter violent extremism, which will be accomplished through existing funding and by prioritizing within the resources available to relevant departments and agencies. Some of these activities are specific to CVE, while others address broader non-security policy objectives but may have an indirect effect on countering radicalization to violence. Because our efforts are threaded across a range of different missions, such as training, outreach, and international exchanges, the execution of the SIP will be impacted by funding for both security and non-security related activities.

Process for Developing the SIP

The Obama Administration continues to prioritize and stress the critical importance of CVE in the Homeland. Given the complexities of addressing this threat and the uniqueness of the operating environment in the United States, the Administration recognizes the potential to do more harm than good if our Nation's approach and actions are not dutifully considered and deliberated. Throughout this process, careful consideration was given to the rule of law and constitutional principles, particularly those that address civil rights and civil liberties. With those principles in mind, we noted that departments and agencies with domestically focused mandates have an array of tools and capabilities that can be leveraged to prevent violent extremism, though some have limited experience in the national security arena. This necessitated a deliberative and carefully calibrated approach with an extensive evaluative period to fully address their potential roles and participation, which for some entailed thinking outside their traditional mandates and areas of work.

After assessing how individuals are radicalized and recruited to violence in the United States, the Administration established an accelerated process, led by the National Security Staff (NSS), to develop the National Strategy for Empowering Local Partners and the SIP. An Interagency Policy Committee (IPC) on countering and preventing violent extremism in the United States was established—with Assistant and Deputy Assistant Secretary-level representatives from across government—to consider roles and responsibilities, potential activities, guiding principles, and how best to coordinate and synchronize our efforts. The IPC, with support from specialist sub-IPCs, drafted our first national strategy on preventing violent extremism in the United States, which was approved by Deputies from the various departments and agencies and signed by the President.

- The following departments and agencies were involved in the deliberations and approval process: the Departments of State (State), the Treasury, Defense (DOD), Justice (DOJ), Commerce, Labor, Health and Human Services (HHS), Education (EDU), Veterans Affairs, and Homeland Security (DHS), as well as the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC).

To develop the SIP, the NSS tasked NCTC with coordinating the first comprehensive baseline of activities across the United States Government related to countering and preventing violent extremism in the United States, which constitutes the ongoing activities outlined in the SIP. This included CVE-specific initiatives, as well as activities that were not developed for CVE purposes, but nonetheless may indirectly contribute to the overall goals of the National Strategy for Empowering Local Partners. These activities were aligned with objectives and sub-objectives—based on the strategy and approved by the IPC—to

assess our overall effort and identify gaps. The IPC then considered ongoing and potential actions to address these gaps, which form the basis of planned activities outlined in the SIP. The SIP was approved by Deputies from the various departments and agencies in November 2011.

Compliance with the Rule of Law

A fundamental precept of the SIP is that the Federal Government's actions must be consistent with the Constitution and in compliance with U.S. laws and regulations. Departments and agencies are responsible for identifying and complying with legal restrictions governing their activities and respective authorities. Compliance with the rule of law, particularly ensuring protection of First Amendment rights, is central to our National Strategy for Empowering Local Partners and the execution of the SIP.

Crosscutting and Supportive Activities

There are fundamental activities that are critical to our success and cut across the objectives of the SIP. These include: (1) whole-of-government coordination; (2) leveraging existing public safety, violence prevention, and community resilience programming; (3) coordination of domestic and international CVE efforts, consistent with legal limits; and (4) addressing technology and virtual space. In many instances, these crosscutting and supportive activities describe the ongoing activities of departments and agencies in fulfilling their broader missions. As they implement new initiatives and programs in support of the SIP, departments and agencies will ensure these enabling activities appropriately guide their efforts.

1. Whole-of-Government Coordination

Leveraging the wide range of tools, capabilities, and resources of the United States Government in a coordinated manner is essential for success. Traditional national security or law enforcement agencies such as DHS, DOJ, and the FBI will execute many of the programs and activities outlined in the SIP. However, as the National Strategy for Empowering Local Partners states, we must also use a broader set of good governance programs, "including those that promote immigrant integration and civic engagement, protect civil rights, and provide social services, which may also help prevent radicalization that leads to violence." To this end, agencies such as EDU and HHS, which have substantial expertise in engaging communities and delivering services, also play a role.

This does not mean the missions and priorities of these partners will change or that their efforts will become narrowly focused on national security. Their inclusion stems from our recognition that radicalization to violence depends on a variety of factors, which in some instances may be most effectively addressed by departments and agencies that historically have not been responsible for national security or law enforcement. These non-security partners, including specific components within DOJ and DHS, have an array of tools that can contribute to this effort by providing indirect but meaningful impact on CVE, including after school programs, networks of community-based organizations that provide assistance to new immigrants, and violence prevention programs. We will coordinate activities, where appropriate, to support the CVE effort while ensuring we do not change the core missions and functions of these departments and agencies.

2. Leveraging Existing Public Safety, Violence Prevention, and Resilience Programming

While preventing violent extremism is an issue of national importance, it is one of many safety and security challenges facing our Nation. As we enter an era of increased fiscal constraints, we must ensure our approach is tailored to take advantage of current programs and leverages existing resources. Our efforts therefore will be supported, where appropriate, by emphasizing opportunities to address CVE within available resources related to public safety, violence prevention, and building resilience.

3. Coordination of Domestic and International Efforts

While always ensuring compliance with applicable laws and regulations, we must ensure a high level of coordination between our domestic and international efforts to address violent extremism. Although both the National Strategy for Empowering Local Partners and the SIP specifically address preventing violent extremism in the United States, the delineation between domestic and international is becoming increasingly less rigid. Violent extremists operating abroad have direct access to Americans via the Internet, and overseas events have fueled violent extremist radicalization and recruitment in the United States. The converse is also true: events occurring in the United States have empowered the propaganda of violent extremists operating overseas. While making certain that they stay within their respective authorities, departments and agencies must ensure coordination between our domestic and international CVE efforts. Given its mandate to support both domestic and international planning, NCTC will help facilitate this part of the CVE effort so that our Homeland and overseas activities are appropriately synchronized, consistent with all applicable laws and regulations. While individual departments and agencies will regularly engage foreign partners, all international engagement will continue to be coordinated through State.

4. Addressing Technology and Virtual Space

The Internet, social networking, and other technology tools and innovations present both challenges and opportunities. The Internet has facilitated violent extremist recruitment and radicalization and, in some instances, attack planning, requiring that we consider programs and initiatives that are mindful of the online nature of the threat. At the same time, the Federal Government can leverage and support the use of new technologies to engage communities, build and mobilize networks against violent extremism, and undercut terrorist narratives. All of our activities should consider how technology impacts radicalization to violence and the ways we can use it to expand and improve our whole-of-government effort. As noted in sub-objective 3.3, we will develop a separate strategy focused on CVE online.

Roles and Responsibilities

The SIP assigns Leads and Partners in each of the Future Activities and Efforts listed under respective sub-objectives. Leads and Partners have primary responsibility for coordinating, integrating, and synchronizing activities to achieve SIP sub-objectives and the overall goal of the National Strategy for Empowering Local Partners.

Expectation of Leads and Partners are as follows:

Lead: A department or agency responsible for convening pertinent partners to identify, address, and report on steps that are being taken, or should be taken, to ensure activities are effectively executed. The Lead is accountable for, among other things:

- Fostering communication among Partners to ensure all parties understand how to complete the activity;
- Identifying, in collaboration with assigned Partners, the actions and resources needed to effectively execute the activity;
- Identifying issues that impede progress; and
- Informing all departments and agencies about the status of progress by the Lead and other sub-objective Partners, including impediments, modifications, or alterations to the plan for implementation.

Partner: A department or agency responsible for collaborating with a Lead and other Partners to accomplish an activity. Partner(s) are accountable for:

- Accomplishing actions under their department or agency's purview in a manner that contributes to the effective execution of an activity;
- Providing status reports and assessments of progress on actions pertinent to the activity; and
- Identifying resource needs that impede progress on their department or agency's activities.

Assessing Progress

It is important to recognize that the National Strategy for Empowering Local Partners represents the first time the United States Government has outlined an approach to address ideologically inspired violent extremism in the Homeland. While the objectives and sub-objectives listed in the SIP represent the collective wisdom and insight of the United States Government about what areas of action have the greatest potential to prevent violent extremism, we will learn more about our effectiveness as we assess our efforts over time, and we will adjust our activities accordingly.

Given the short history of our coordinated, whole-of-government approach to CVE, we will first develop key benchmarks to guide our initial assessment. Where possible, we will also work to develop indicators of impact to supplement these performance measures, which will tell us whether our activities are having the intended effects with respect to an objective or sub-objective. As we implement our activities, future evaluations will shift away from benchmark performance measures towards impact assessments. Departments and agencies will be responsible for assessing their specific activities in pursuit of SIP objectives, in coordination with an Assessment Working Group. We will develop a process for identifying gaps, areas of limited progress, resource needs, and any additional factors resulting from new information on the dynamics of radicalization to violence. Our progress will be evaluated and reported annually to the President.

Objectives, Sub-Objectives, and Activities

The SIP's objectives mirror the National Strategy for Empowering Local Partners' areas of priority action: (1) enhancing Federal engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals. Each of these is supported by sub-objectives, which constitute measurable lines of effort with which our specific programs and initiatives are aligned. A key purpose of the SIP is to describe the range of actions we are taking to improve or expand these efforts.

1. Enhancing Federal Engagement with and Support to Local Communities that May be Targeted by Violent Extremists

Communication and meaningful engagement with the American public is an essential part of the Federal Government's work, and it is critical for developing local partnerships to counter violent extremism. Just as we engage and raise awareness to prevent gang violence, sexual offenses, school shootings, and other acts of violence, so too must we ensure that our communities are empowered to recognize threats of violent extremism and understand the range of government and nongovernment resources that can help keep their families, friends, and neighbors safe. As noted in the National Strategy for Empowering Local Partners:

> Engagement is essential for supporting community-based efforts to prevent violent extremism because it allows government and communities to share information, concerns, and potential solutions. Our aims in engaging with communities to discuss violent extremism are to: (1) share sound, meaningful, and timely information about the threat of violent extremism with a wide range of community groups and organizations, particularly those involved in public safety issues; (2) respond to community concerns about government policies and actions; and (3) better understand how we can effectively support community-based solutions.

At the same time, we must ensure that our efforts to prevent violent extremism do not narrow our relationships with communities to any single issue, including national security. This necessitates continuing to engage on the full range of community interests and concerns, but it also requires, where feasible, that we incorporate communities that are being targeted by violent extremists into broader forums with other communities when addressing non-CVE issues. While we will engage with some communities specifically on CVE issues because of particular needs, care should be taken to avoid giving the false impression that engagement on non-security issues is taking place exclusively because of CVE concerns. To ensure transparency, our engagement with communities that are being targeted by violent extremists will follow two tracks:

- We will specifically engage these communities on the threat of violent extremism to raise awareness, build partnerships, and promote empowerment. This requires specific conversations and activities related to security issues.
- Where we engage on other topics, we will work to include them in broader forums with other communities when appropriate.

1.1 Improve the depth, breadth, and frequency of Federal Government engagement with and among communities on the wide range of issues they care about, including concerns about civil rights, counterterrorism security measures, international events, and foreign policy issues.

Violent extremist narratives espouse a rigid division between "us" and "them" that argues for exclusion from the broader society and a hostile relationship with government and other communities. Activities that reinforce our shared sense of belonging and productive interactions between government and the people undercut this narrative and emphasize through our actions that we are all part of the social fabric of America. As President Obama emphasized, when discussing Muslim Americans in the context of al-Qa'ida's attempts to divide us, "we don't differentiate between them and us. It's just us."

Current Activities and Efforts

Departments and agencies have been conducting engagement activities based on their unique mandates. To better synchronize this work, U.S. Attorneys, who historically have engaged with communities in their districts, have begun leading Federal engagement efforts. This includes our efforts to engage with communities to (1) discuss issues such as civil rights, counterterrorism security measures, international events, foreign policy, and other community concerns; (2) raise awareness about the threat of violent extremism; and (3) facilitate partnerships to prevent radicalization to violence. The types of communities involved in engagement differ depending on the locations. United States Attorneys, in consultation with local and Federal partners, are best positioned to make local determinations about which communities they should engage. Appointed by the President and confirmed by the Senate, U.S. Attorneys are the senior law enforcement and executive branch officials in their districts, and are therefore well-placed to help shape and drive community engagement in the field.

In December 2010, 32 U.S. Attorneys' Offices began expanding their engagement with communities to raise awareness about how the United States Government can protect all Americans from discrimination, hate crimes, and other threats; to listen to concerns; and to seek input about government policies and programs. In some instances, these efforts also included initiatives to educate the public about the threat of violent extremist recruitment, which is one of many components of a broader community outreach program.

- During this initial pilot, these U.S. Attorneys significantly expanded outreach and engagement on a range of issues of interest to communities; built new relationships where needed; and communicated the United States Government's approach to CVE.
- Departments and agencies, including State, the Treasury, EDU, HHS, and DHS provided information, speakers, and other resources for U.S. Attorneys' community engagement activities, frequently partnering with DOJ on specific programs and events.

A National Task Force, led by DOJ and DHS, was established in November 2010 to help coordinate community engagement at the national level. It includes all departments and agencies involved in relevant community engagement efforts and focuses on compiling local, national, and international best practices and disseminating these out to the field, especially to U.S. Attorneys' Offices. The Task Force is also responsible for connecting field-based Federal components to the full range of United States Government officials involved in community engagement to maximize partnerships,

coordination, and resource-sharing. The following are some examples of engagement efforts that are, or will be, coordinated with the Task Force:

- The DHS Office for Civil Rights and Civil Liberties (CRCL) this year doubled its outreach to communities and expanded its quarterly engagement roundtables to 14 cities throughout the country. During Fiscal Year 2011, CRCL also conducted 72 community engagement events, some of which included CVE-related topics.
- State engaged on U.S. foreign policy with a range of interested domestic communities. The Bureau of Near Eastern Affairs alone conducted 80 outreach events over the past year.
- DOJ has produced a number of brochures and other materials on civil rights protections and steps individuals can take to prevent or respond to discrimination, and has disseminated these to various communities, including those being targeted by violent extremists. DOJ has translated these materials into a number of languages, including Arabic, Somali, Urdu, Farsi, and Hindi.
- DOJ, in coordination with DHS, expanded the Building Communities of Trust (BCOT) Initiative, which focuses on developing relationships among local law enforcement departments, fusion centers, and the communities they serve to educate communities on: (1) the Nationwide Suspicious Activity Reporting Initiative (NSI); (2) how civil rights and liberties are protected; and (3) how to report incidents in order to help keep our communities safe. DOJ continues to support the BCOT Initiative.

Future Activities and Efforts

The primary focus for the next year will be: (1) expanding the scope of engagement; (2) building new partnerships between communities and local law enforcement, local government officials, and civil society; (3) incorporating communities that are being targeted by violent extremist radicalization into broader forums with other communities to engage on a range of non-security issues; and (4) increasing our engagement specifically on CVE. Additional activities going forward include the following:

- DOJ will incorporate more U.S. Attorneys' Offices as engagement leads in the field, building on the initial U.S. Attorney-led effort. (Lead: DOJ; Partners: All)
- The National Task Force will: (1) disseminate regular reports on best practices in community engagement to local government officials, law enforcement, U.S. Attorneys' Offices, and fusion centers; (2) work with departments and agencies to increase their support to U.S. Attorney-led engagement efforts in the field; and (3) closely coordinate Federal engagement efforts with communities targeted by violent extremist radicalization. (Leads: DOJ and DHS; Partners: All)
- In consultation with Federal and local partners, the National Task Force and the U.S. Attorneys' Offices will facilitate, where appropriate, the inclusion of communities that may be targeted by violent extremist radicalization into broader engagement forums and programs that involve other communities. (Leads: DOJ and DHS; Partners: All)
- U.S. Attorneys will coordinate closely with local government officials, law enforcement, communities, and civil society to enhance outreach events and initiatives. (Lead: DOJ; Partners: All)

- In Fiscal Year (FY) 2012, CRCL plans on expanding its quarterly community engagement roundtables to a total of 16. CRCL is also in the process of implementing a campus youth community engagement plan, through which it will engage with young adults on the topic of violent extremism. (Lead: DHS)
- Depending on local circumstances, and in consultation with the FBI and other agencies as appropriate, U.S. Attorneys will coordinate any expanded engagement specific to CVE with communities that may be targeted by violent extremist radicalization. (Lead: DOJ; Partners: DHS, NCTC, and FBI)
- An FBI CVE Coordination Office will be established and, as part of its activities, will coordinate with the National Task Force on CVE-specific education and awareness modules. These modules will be developed and implemented, in part, by leveraging some of the FBI's existing programs and initiatives. (Lead: FBI; Partners: DOJ and DHS)
- DHS will oversee an online portal to support engagement by government officials and law enforcement with communities targeted by violent extremist radicalization, which will be used to share relevant information and build a community of interest. The portal will be accessible to government officials and law enforcement involved in overseas and domestic CVE and community engagement efforts to share best practices. (Lead: DHS; Partners: State, and NCTC)
- DOJ will expand the efforts of the BCOT initiative to help facilitate trust between law enforcement and community leaders. This dialogue could include local issues, as well as CVE. (Lead: DOJ; Partner: DHS)
- The United States Government will build a digital engagement capacity in order to expand, deepen, and intensify our engagement efforts. Where possible, virtual engagement will build on real world engagement activities and programs. (Lead: DHS; Partners: All)

1.2 *Foster community-led partnerships and preventative programming to build resilience against violent extremist radicalization by expanding community based solutions; leveraging existing models of community problem-solving and public safety; enhancing Federal Government collaboration with local governments and law enforcement to improve community engagement and build stronger partnerships; and providing communities with information and training, access to resources and grants, and connections with the philanthropic and private sectors.*

The Federal Government can foster nuanced and locally rooted counter-radicalization programs and initiatives by serving as a facilitator, convener, and source of information to support local networks and partnerships at the grassroots level. Importantly, because the dynamics of radicalization to violence frequently vary from location to location, we recognize that a one-size-fits-all approach will be ineffective.

Current Activities and Efforts

The Federal Government has held a series of consultative meetings with communities, local government and law enforcement, civil society organizations, foundations, and the private sector to better understand how it can facilitate partnerships and collaboration. This leverages a key strength identified

in the National Strategy for Empowering Local Partners: "The Federal Government, with its connections to diverse networks across the country, has a unique ability to draw together the constellation of previously unconnected efforts and programs to form a more cohesive enterprise against violent extremism." Examples of this include the following:

- DHS Secretary Napolitano tasked her Homeland Security Advisory Council (HSAC) to develop recommendations on how the Department can best support law enforcement and communities in their efforts to counter violent extremism. An HSAC CVE Working Group convened multiple meetings with local law enforcement, local elected officials, community leaders (including faith-based leaders), and academics. The working group released its recommendations in August 2010, highlighting the importance of: (1) research and analysis of violent extremism; (2) engagement with communities and leveraging existing partnerships to develop information-driven, community-based solutions to violent extremism and violent crime; and (3) community oriented policing practices that focus on building partnerships between law enforcement and communities.
- DHS and NCTC began raising awareness about violent extremism among private sector actors and foundations and connected them with community civic activists interested in developing programs to counter violent extremism. DHS is now working with a foundation to pilot resiliency workshops across the country that address all hazards, including violent extremism.

We also began exploring how to incorporate CVE as an element of programs that address broader public safety, violence prevention, and resilience issues. This has the advantage of leveraging preexisting initiatives and incorporates CVE in frameworks (such as safeguarding children) used by potential local partners who may otherwise not know how they fit into such efforts. For example, although many teachers, healthcare workers, and social service providers may not view themselves as potentially contributing to CVE efforts, they do recognize their responsibilities in preventing violence in general. CVE can be understood as a small component of this broader violence prevention effort. Departments and agencies will review existing public safety, violence prevention, and resilience programs to identify ones that can be expanded to include CVE as one among a number of potential lines of effort.

- As an example, the Federal Government helped support a community-led initiative to incorporate CVE into a broader program about Internet safety. The program addressed protecting children from online exploitation, building community resilience, and protecting youth from Internet radicalization to violence.

Future Activities and Efforts

Planned activities to expand support to local partners include the following:

- The Federal Government will help broker agreements on partnerships to counter violent extremism between communities and local government and law enforcement to help institutionalize this locally focused approach. (Lead: DHS)
- DHS and DOJ will work to increase support for local, community-led programs and initiatives to counter violent extremism, predominantly by identifying opportunities within existing appropriations for incorporating CVE as an eligible area of work for public safety, violence prevention, and community resilience grants. (Leads: DHS and DOJ)

- DHS is working to increase funding available to integrate CVE into existing community-oriented policing efforts through FY12 grants. (Lead: DHS)
- DHS is establishing an HSAC Faith-Based Community Information Sharing Working Group to determine how the Department can: (1) better share information with faith communities; and (2) support the development of faith-based community information sharing networks. (Lead: DHS)
- DHS is developing its Hometown Security webpage to include resources such as training guidance, workshop reports, and information on CVE for both the general public and law enforcement. (Lead: DHS)
- The Treasury will expand its community outreach regarding terrorism financing issues. (Lead: Treasury; Partners: State, DOJ, DHS, FBI, and the U.S. Agency for International Development)[3]
- Depending on local circumstances and in consultation with the FBI, U.S. Attorneys will coordinate, as appropriate, any efforts to expand connections and partnerships at the local level for CVE, supported by the National Task Force where needed. (Lead: DOJ; Partners: All)
- Departments and agencies will expand engagement with the business community by educating companies about the threat of violent extremism and by connecting them to community civic activists focused on developing CVE programs and initiatives. (Lead: DHS; Partner: NCTC)

2. Building Government and Law Enforcement Expertise for Preventing Violent Extremism

It is critical that the Federal Government and its local government and law enforcement partners understand what the threat of violent extremism is, and what it is not. This helps ensure that we focus our resources where they are most effective and that we understand how we can best empower and partner with communities. Building expertise necessitates continued research about the dynamics of radicalization to violence and what has worked to prevent violent extremism; sharing this information as widely as possible; and then leveraging it to train government officials and law enforcement.

2.1 Improve our understanding of violent extremism through increased research, analysis, and partnerships with foreign governments, academia, and nongovernmental organizations.

The Federal Government has built a robust analytic program to understand violent extremism that includes analysis; research conducted by academia, think tanks, and industry; and exchanges with international allies to identify best practices. While we have increased our understanding of how individuals are radicalized to violence, we must continue to identify gaps, monitor changes in the dynamics of violent extremism, and remain vigilant by challenging our assumptions and continuing our research and analysis.

Current Activities and Efforts

The United States Government's research capacity on this issue has greatly expanded. DHS and NCTC both have analytic groups exclusively focused on violent extremist radicalization; the Interagency Intelligence Subcommittee on Radicalization helps coordinate and improve CVE intelligence analysis; and we work with foreign governments, academia, and nongovernmental organizations to inform and

[3] The U.S. Agency for International Development's role will be limited to sharing relevant information.

supplement our analysis and understanding. In addition to a large volume of intelligence products on CVE, examples of activities include:

- DHS Science & Technology (S&T) sponsored research on violent extremism in the United States, which it has shared with DHS components and other departments and agencies. Over 20 reports have been produced since 2009 and 5 more will be produced by the end of 2011. DHS is also developing an integrated open source database to help inform CVE programs.
- DHS's Office of Intelligence and Analysis (I&A) collaborated with the FBI, the Bureau of Prisons (BOP), and NCTC to assess the capacity of state correctional institutions to detect and share information regarding individuals who demonstrate behaviors associated with violent extremism while in the correctional system.
- The National Intelligence Council, DHS, FBI, and NCTC briefed fusion centers and law enforcement around the country on violent extremism.
- DHS, in partnership with the FBI and NCTC, developed case studies on preoperational indicators and known threats for State and local law enforcement and affected communities.
- The United States Government held regular exchanges of best practices with Australia, Canada, Denmark, Germany, the European Union, the Netherlands, the United Kingdom, and other partners to gain comparative insights about what might be effective in the Homeland.
- DHS expanded cooperation between the United States and Canada on CVE research and lessons learned.
- The United States Government participates in the Global Counterterrorism Forum's CVE Working Group.
- As directed in the Fort Hood Follow-on Review, DOD established the Force Protection Senior Steering Group. Among the Steering Group's duties is the coordination of non-traditional partners' activities within DOD (e.g., counterintelligence and behavioral health) to better understand how to identify and prevent all forms of violent extremism—not limited to al-Qa'ida-inspired extremism—within the military, including the potential use of DOD's extensive network of programs designed to support individuals who are potentially at risk of committing acts of violence against themselves, their families, or co-workers.

Future Activities and Efforts

Although we have a better understanding of the threat, there are gaps that need to be addressed through additional research and analysis. In this regard, we will:

- Expand analysis in five priority areas (Leads: DHS, FBI, NCTC, and State):
    1. The role of the Internet in radicalization to violence and how virtual space can be leveraged to counter violent extremism.
    2. Single-actor terrorism (so called "lone wolves"), including lessons learned from similar phenomena such as a school shooters.
    3. Disengagement from terrorism and violent extremism.

4. Non-al-Qa'ida related radicalization to violence and anticipated future violent extremist threats.
5. Preoperational indicators and analysis of known case studies of extremist violence in the United States.

- Continue DHS S&T's support for research on countering the threat of extremist violence. (Lead: DHS)
- Continue DHS collaboration with the FBI, the BOP, and NCTC to: (1) improve awareness of the risk of violent extremism in correctional systems; (2) enhance screening of new inmates to detect individuals associated with violent extremist organizations; (3) improve detection of recruitment efforts within the correctional environment; and (4) increase information sharing, as appropriate, with Federal, State, and local law enforcement about inmates who may have adopted violent extremist beliefs and are being released. (Lead: DHS; Partners: DOJ, FBI, and NCTC)
- Complete the creation of the FBI CVE Coordination Office to help assess and leverage existing Bureau efforts to better understand and counter violent extremism. (Lead: FBI)
- Build lines of research specifically to support non-security Federal partners. (Leads: DHS and NCTC; Partners: EDU and HHS)

2.2 Increase Federal Government information sharing with State, local, and tribal governments and law enforcement on terrorist recruitment and radicalization.

As we enhance our partnerships with State, local, and tribal governments and law enforcement to counter violent extremism, it is essential that we share our expertise and insights about the dynamics of radicalization to violence and what has worked to prevent it. This, in turn, will help our partners identify potential areas of collaboration with communities and other local actors.

Current Activities and Efforts

Examples include:

- Based on direction from the Office of the Director of National Intelligence (DNI), DHS led an effort to improve the analysis of homegrown violent extremism, including analytic tools to share with State, local, and tribal partners. DHS briefed representatives of 47 states on the project.
- DHS generated case studies of known and suspected terrorists and assessments of radicalization to violence, based on recent arrests, to share with local partners.
- FBI disseminated information to public safety partners, including information about radicalization to violence.
- DHS, NCTC, and FBI briefed and disseminated information on how individuals are radicalized to violence to law enforcement, fusion centers, and local government officials, including the Major Cities Chiefs, representatives from 47 states, Mayors' Offices, and State Homeland Security Advisors.

- In partnership with NCTC, DOJ, DNI, and FBI, DHS led the first National CVE Workshop in August 2011, which brought together intelligence commanders from major metropolitan areas and fusion center directors to increase their understanding of CVE.

Future Activities and Efforts

More work needs to be done to ensure our State, local, and tribal partners have the information they need to counter violent extremism. Classification remains an obstacle to broader sharing with these partners, but we can better ensure that analytic production is tailored to the needs of practitioners in the field. Major work over the next year will focus on creating more analytic products on CVE that directly support local law enforcement and government. Planned actions include:

- Development of an analytic team focused on supporting local government and law enforcement CVE practitioners and increased production of analysis at appropriate classification levels. (Lead: DHS; Partners: FBI and NCTC)
- Development of practitioner-friendly summaries of current research and literature reviews about the motivations and behaviors associated with single-actor terrorism and disengagement from violent extremism. (Lead: DHS)
- Review of information-sharing protocols to identify ways of increasing dissemination of products to State, local, and tribal authorities. (Leads: DHS, DOJ, FBI, and NCTC)
- Expansion of briefings and information sharing about violent extremism with State and local law enforcement and government. (Lead: DHS, FBI, and NCTC)

2.3 *Improve the development and use of standardized training with rigorous curricula based on the latest research, which conveys information about violent extremism; improves cultural competency; and imparts best practices and lessons learned for effective community engagement and partnerships.*

The Federal Government has expanded and improved training related to CVE over the past year, but challenges remain. In particular, there is a need for a review process and standards for training specific to CVE, which was underscored by a small number of instances of Federally sponsored or funded CVE-related and counterterrorism training that used offensive and inaccurate information, which was inconsistent with our values and core principles. As our National Strategy to Empower Local Partners highlights, "Misinformation about the threat and dynamics of radicalization to violence can harm our security by sending local stakeholders in the wrong direction and unnecessarily creating tensions with potential community partners." Therefore, improving Federal Government-approved training practices and processes related to CVE is a top priority of this plan.

Current Activities and Efforts

In November 2010, the IPC tasked DHS to form an Interagency Working Group on Training to catalogue and recommend improvements for CVE-related training across government. The Working Group brought together individuals responsible for CVE training and substantive specialists from civil rights and civil liberties offices, Federal law enforcement, and the analytic community. This is part of our overall

emphasis on improving the quality and quantity of CVE-related training. Notable accomplishments in our efforts to improve training include:

- Between October 2010 and October 2011, DHS CRCL trained nearly 2,700 law enforcement officials on CVE and cultural awareness at 46 separate events. The training served as the basis for best practices recommended by the Interagency Working Group on Training.
- Based on input from participating agencies, DHS issued CVE training guidance and best practices in October 2011 for Federal, State, local, and tribal government officials charged with organizing training related to CVE, cultural awareness, and counterterrorism.
- The Federal Emergency Management Agency (FEMA) in October 2011 issued an Information Bulletin on CVE Training, which includes DHS's training guidance and best practices, as well as guidance for State, local, and tribal entities that regularly leverage FEMA grants to fund CVE-related trainings. DHS sent the best practices paper and the FEMA guidance to all DHS grantees, State and local governments, State and local law enforcement, relevant community stakeholders, and interagency partners.
- DHS provided a full-day of training, which included training on cultural competency, civil rights, and civil liberties to Federal, State, local, and tribal partners at 12 fusion centers in the past year and over 30 fusion centers since 2008. These trainings were coupled with 3- to 4-hour CVE training sessions for State and local law enforcement operating in the same state. Additionally, DHS provided "train the trainer" sessions for staff from nearly all fusion centers nationwide.
- DHS, working closely with other departments and agencies, local law enforcement, academics, and curriculum development experts, developed guidelines for a CVE curriculum that focuses on information-driven community-oriented policing practices and how to leverage existing community partnerships to counter violent extremism and violent crime. These guidelines were reviewed and validated in February 2011 at a "proof-of-concept" session at the Federal Law Enforcement Training Center (FLETC), which was attended by State, local, and tribal law enforcement executives and frontline officers from rural and major city jurisdictions.
- State, working closely with NCTC and DHS, piloted specialized CVE training for United States Government officials working on CVE in the United States and abroad through its Foreign Service Institute in May 2011. Participation by domestic and international practitioners provided opportunities for exchanging best practices, enhanced the coordination of our Homeland and overseas efforts, and encouraged interagency partnerships.

Future Activities and Efforts

A review process by the Interagency Working Group on Training, as well as internal assessments by departments and agencies, indentified two key challenges, which we will address over the next year:

- Many departments and agencies lack a review process for training materials and outside speakers on CVE, which led to a small number of cases of training that violated internal principles as well as core tenets of the National Strategy to Empower Local Partners.

- There has been a lack of guidance and standards for training related to CVE, which left field offices, in particular, vulnerable to bad training. Without guidance or standards, it has been difficult to enforce accountability.

We have prioritized addressing these two shortcomings by doing the following:

- Departments and agencies are taking steps to identify training materials that may not meet internal standards and to improve processes for creating and reviewing such materials. Some departments are consulting with outside experts with established reputations to evaluate the content and training review process. Guidance on CVE-related training is being developed and will be issued, both across the organizations and to field components. Some departments may issue this as part of broader training guidance. (Lead: All)
- DHS, via FLETC, is in the process of developing a CVE curriculum to be integrated into existing training programs for Federal law enforcement. The curriculum will give Federal law enforcement a better understanding of CVE and how to more effectively leverage existing local partnerships. (Lead: DHS)
- DHS is in the process of establishing an internal committee to review all directly funded and issued DHS training on cultural competency, engagement, CVE, and counterterrorism. The committee will be responsible for reviewing any new content, evaluating experts, and establishing quality control. FEMA will incorporate the recently released Informational Bulletin and training guidance into FY12 grant guidance and will also leverage existing mechanisms to hold grantees and sub-grantees accountable. (Lead: DHS)

In addition to addressing the quality issue, we will work to expand the quantity of training.

- DHS, in partnership with the Los Angeles Police Department and the National Consortium for Advanced Policing, is developing a CVE curriculum that includes a 16-hour continuing education module for executive and frontline officers, as well as a 30-minute module that will be introduced at police academies. Both will be certified by the Police Officers Standards and Training Council. In October 2011 the Major Cities Chiefs Association passed a motion to adopt and implement the DHS CVE curriculum, which will be piloted with State and local law enforcement in San Diego by the end of 2011. By 2013, DHS seeks to: (1) implement the curriculum across the country on a regional basis; (2) develop a national network of trainers and subject matter experts who can administer the training and keep it current; and (3) build an online component for the curriculum. (Lead: DHS; Partners: DOJ and NCTC)
- DHS, via FLETC, will update current Federal training programs to integrate the CVE curriculum for Federal law enforcement in the coming year. (Lead: DHS)
- DHS is working with European law enforcement partners to share best practices and case studies to improve training, community policing, and operational information sharing. (Lead: DHS)
- DHS CRCL is expanding and institutionalizing its CVE and cultural competence training curricula to further enhance the material and its effectiveness. (Lead: DHS)

- The Interagency Working Group on Training will facilitate a "train the trainer program" to increase the reach of CVE training. (Leads: DHS and NCTC; Partners: DOJ, EDU, HHS, and FBI)
- The Interagency Working Group on Training will facilitate the development of an online training program that provides professional development credit for a broad range of professions, particularly those involved with public safety, violence prevention, and resilience. This will help build a basic understanding of CVE among a broad cross-section of stakeholders who have related mandates. (Leads: DHS and NCTC; Partners: DOJ, FBI, EDU, and HHS)
- The Interagency Working Group on Training will collaborate with non-security partners, such as EDU, to build CVE training modules that can be incorporated, as appropriate, into existing programs related to public safety, violence prevention, and resilience. These modules will be crafted in a way that is relevant to the specific audiences and their missions. Only trainers who have undergone CVE-specific training will deliver training programs that include CVE modules. (Lead: DHS; Partners: DOJ, EDU, HHS, FBI, and NCTC)
- DOD's training programs and curricula will be informed by the work of the Interagency Working Group on Training, as appropriate. Additionally, DOD is conducting a review of CVE-related curricula and will make revisions and adjustments as necessary. (Lead: DOD; Partner DHS)

3. Countering violent extremist propaganda while promoting our ideals

As the National Counterterrorism Strategy emphasizes, "[t]he United States was founded upon a belief in a core set of values that is written into our founding documents and woven into the very fabric of our society. Where terrorists offer injustice, disorder, and destruction the United States must stand for freedom, fairness, equality, dignity, hope, and opportunity. The power and appeal of our values enables the United States to build a broad coalition to act collectively against the common threat posed by terrorists, further delegitimizing, isolating, and weakening our adversaries."

Countering the ideologies and narratives that legitimize violence is central to our effort, but it also is the most challenging area of work, requiring careful consideration of a number of legal issues, especially those related to the First Amendment. In many instances, it will be more effective to empower communities to develop credible alternatives that challenge violent extremist narratives rather than having the Federal Government attempt to do so.

Our efforts include not only challenging justifications for violence, but affirming American ideals of inclusiveness and opportunity as well. Violent extremist narratives feed on disenchantment and the sense of exclusion. Our efforts therefore must include positive affirmation of our unity as a country. To some extent, this is addressed through our engagement activities, particularly where they address challenges facing all communities and not just those targeted by violent extremist radicalization. But there are also situations where we will need to more directly challenge violent extremist narratives.

3.1 Increase the capacity of communities to directly challenge violent extremist ideologies and narratives.

While the government cannot always directly contest violent extremist ideas, it can support capacity building within communities to take on this role. Whereas sub-objective 1.2 emphasizes preventative

measures and a defensive posture to build capacity for enhancing community resilience, sub-objective 3.1 focuses on increasing the ability of communities to push back against violent extremist propaganda.

Current Activities and Efforts

Most of our work in this area to date has focused on connecting community activists to potential civil society and private sector partners to focus specifically on undermining violent extremist narratives. Over the past year, we have taken the following steps:

- NCTC in 2010 developed a Community Awareness Briefing (CAB) to inform members of the public about efforts by al-Qa'ida and its adherents and affiliates to recruit Americans. The CAB highlights recruiting videos and examples of violent extremist propaganda, while underscoring the fact that these materials are often easily available on the Internet. Most importantly, the CAB aims to facilitate a discussion about what government and communities can do, together and independently, to counter the threat of violent extremist narratives. NCTC continues to deliver the presentation at forums composed of community leaders, educators, and parents in cities across the United States. In March 2011, NCTC held a workshop for local, State, and field-based Federal officials on how the CAB could be used in engagement efforts, when it makes sense and is appropriate.
- NCTC connected civic activists with technology experts, resulting in a training seminar on how to maximize the use of technology to counter violent extremism online.
- State sponsored speaker series and exchanges between international CVE practitioners and American communities targeted by violent extremist recruiters to better understand effective models for countering violent extremist narratives.

Future Activities and Efforts

This is a nascent area of effort and therefore will necessitate greater focus over the next year. Our planned actions include:

- Expanding efforts to raise community awareness about the threat of radicalization to violence, building from the experience of the CAB, and adapting those materials for different audiences where appropriate. (Leads: DOJ, DHS, FBI, and NCTC)
- Learning from former violent extremists, specifically those who can speak credibly to counter violent narratives, provide insights to government, and potentially catalyze activities to directly challenge violent extremist narratives. (Lead: DHS; Partner: NCTC)
- Providing grants to counter violent extremist narratives and ideologies, within authorities and relevant legal parameters, by reprioritizing or increasing the flexibility of existing funding. (Lead: DHS)
- Brokering connections between private sector actors, civil society, and communities interested in countering violent extremist narratives. (Lead: DHS; Partner: NCTC)
- Promoting international exchange programs to build expertise for countering violent extremist narratives. (Lead: State; Partners: DDJ, DHS, FBI, and NCTC)

- Increasing technical training to empower communities to counter violent extremists online, including the development of training for bloggers. (Lead: DHS; Partners: State, NCTC, and FBI)

3.2 Improve and increase our communication to the American public about the threat posed by violent extremist groups, myths and misperceptions about violent extremist radicalization, and what we are doing to counter the threat.

It is important that we communicate to the American public the realities of what the threat is, and what it is not. Misconceptions about the threat and statements and actions that cast suspicion on entire communities based on the actions of a few distract attention from the real threat and can undermine our ability to build partnerships. An informed citizenry enhances our national security.

Current Activities and Efforts

In 2011, the Federal Government focused on developing its approach to domestic CVE and communicating this to the American public. This involved briefings to Congress, public addresses, and media interviews. We will continue these activities.

Future Activities and Efforts

In 2012, we will work to expand our efforts to raise awareness in the general public about radicalization to violence in the United States and the tools to prevent it by:

- Providing regular briefings to Congress, think tanks, and members of the media. (Lead: DHS; Partners: DOJ, FBI, and NCTC)
- Creating programs to directly engage the public on the issue. (Lead: All)
- Building a public website on community resilience and CVE. (Lead: DHS)

3.3 Build a strategy to leverage new technologies and address online violent extremist radicalization

The Internet has become an increasingly potent element in radicalization to violence, enabling violent extremists abroad to directly communicate to target audiences in the United States. This direct communication allows violent extremists to bypass parents and community leaders. The SIP specifically addresses the online arena in several sub-objectives, but because of the importance of the digital environment, we will develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience that considers: (1) the latest assessment of the role of the Internet; (2) the absence of clear national boundaries in online space and the relationship between international and domestic radicalization to violence; (3) relevant legal issues; and (4) the differing authorities and capabilities of departments and agencies.

Conclusion

Protecting our Nation's communities from violent extremist recruitment and radicalization is a top national security priority. It is an effort that requires creativity, diligence, and commitment to our fundamental rights and principles. In his cover letter to the National Strategy for Empowering Local Partners, President Obama wrote:

> Sadly, the threat of violent extremism in America is nothing new. Throughout our history, misguided groups—including international and domestic terrorist organizations, neo-Nazis and anti-Semitic hate groups—have engaged in horrific violence to kill our citizens and threaten our way of life. Most recently, al-Qa'ida and its affiliates have attempted to recruit and radicalize people to terrorism here in the United States, as we have seen in several plots and attacks, including the deadly attack 2 years ago on our service members at Fort Hood. As a government, we are working to prevent all types of extremism that leads to violence, regardless of who inspires it.
>
> —President Barack Obama, August 3, 2011

A complex issue like violent extremist radicalization and recruitment requires a nuanced path to guide a whole-of-government approach. The SIP outlines this path and facilitates a division of labor by assigning responsibilities between Federal Government departments, agencies, and components focused on law enforcement and national security and those whose efforts support, but do not directly lie within, these areas.

4 page draft "BM for faith based meeting:

Page 1 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 4 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: Houser, Jason (b)(6)
(b)(6)
To: "Braun, Jacob <(b)(6)
(b)(6)
"Mabeus, Steve
(b)(6)
(b)(6)
(b)(6)
"Duggan, Alaina
(b)(6)
"Saupp, Kevin <
CC: "Snyder, Nathaniel <(b)(6)
(b)(6)
Subject: Re: Time Sensitive Request - CVE Session at the NFCTE
Date: 2012/03/08 10:11:11
Type: Note

Jason P Houser
Intelligence Director - In Support of the Counterterrorism Coordinator
(b)(6)

From: Houser, Jason
Sent: Thursday, March 08, 2012 10:10 AM
To: Braun, Jacob; Mabeus, Steven; (b)(6) Saupp, Kevin
Subject: Re: Time Sensitive Request - CVE Session at the NFCTE

Nate and Alaina and I huddled this morning.

John will be staffing S1 during the Conference.

(b)(6) plan for a panel - minus John - will be what we will need you to work towards

Jason P Houser
Intelligence Director - In Support of the Counterterrorism Coordinator
(b)(6)

From: Braun, Jacob
Sent: Thursday, March 08, 2012 10:06 AM
To: Houser, Jason; Mabeus, Steven; (b)(6) Duggan, Alaina; Saupp, Kevin
Subject: Re: Time Sensitive Request - CVE Session at the NFCTE

Sure. (b)(6) will call you in a few to discuss. What is deadline to figure this out? Today?

From: Houser, Jason
Sent: Thursday, March 08, 2012 06:42 AM
To: Mabeus, Steven; (b)(6) Braun, Jacob; Duggan, Alaina; Saupp, Kevin
Subject: RE: Time Sensitive Request - CVE Session at the NFCTE

Kevin, Jake and Alaina –

We all have been swirling around on this with Steve, Brad, and John.

Lets all chat today so we are on the same page

JPH

From: Mabeus, Steven
Sent: Thursday, March 08, 2012 6:18 AM
To: (b)(6) Braun, Jacob
Cc: Houser, Jason
Subject: FW: Time Sensitive Request - CVE Session at the NFCTE

Please figure this out and clear the panel members with Kevin and John

thanks

From: Saupp, Kevin
Sent: Thursday, March 08, 2012 2:25 AM
To: Mabeus, Steven
Cc: (b)(6) Byrd, William
Subject: RE: Time Sensitive Request - CVE Session at the NFCTE

Maybe a JRIC analyst? the other two from Columbus either are in process of moving to ITACG or already moved to NCTC...

From: Mabeus, Steven
Sent: Wednesday, March 07, 2012 8:46 PM
To: Saupp, Kevin
Cc: Parker, Bradford; Byrd, William
Subject: Re: Time Sensitive Request - CVE Session at the NFCTE

Got any suggestions?
I have no preferences

From: Saupp, Kevin
Sent: Wednesday, March 07, 2012 07:06 PM
To: Mabeus, Steven
Cc: (b)(6) Byrd, William; Duggan, Alaina
Subject: RE: Time Sensitive Request - CVE Session at the NFCTE

(b)(5)

From: Mabeus, Steven (b)(6)
Sent: Wednesday, March 07, 2012 5:14 PM
To: Diane Ragans

Cc: (b)(6) ; Byrd, William
Subject: RE: Time Sensitive Request - CVE Session at the NFCTE

Diane
Here is our info for this session. We are in the process of locking in the panel members now and will have this complete tomorrow. (b)(6) s your POC to complete this action.

Thanks
Steve

Session Overview:
Last December, the White House released its Strategic Implementation Plan to Counter Violent Extremism. The program describes the CVE roles and functions at the Federal, State and local level. The SIP directs Federal Government activity in three specific areas: enhancing engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals. Local officials and authorities in many cities have begun to implement training and outreach efforts tailored for their specific communities.

Take Aways:

- The session will provide an overview of the Strategic Implementation Plan key objectives and activities.
- The session will provide an overview of federal engagement activities and strategies.
- The session will provide lessons learned from long standing programs and introduce new strategies to engage these communities.

Panel Speakers (all tentative but will confirm tomorrow)
John Cohen—Moderator, DHS
Dan Sutherland, NCTC
(b)(7)(C)

From: Diane Ragans (b)(6)
Sent: Wednesday, March 07, 2012 1:51 PM
To: Mabeus, Steven
Subject: Time Sensitive Request - CVE Session at the NFCTE
Importance: High

Hi Steve. I left you a voice mail about this session a short time ago.

(b)(5)

- The speakers and moderator/facilitator for this session should be finalized and their names and contact information forwarded to me.
- The session overview needs to be finalized, to include three brief takeaways. The takeaways should be written based on what an attendee can expect to learn from the presentation.
- A short bio (one or two paragraphs) on each panelist should be submitted as soon as possible.
- As soon as the speakers names and contact information is provided, we will check to make sure they are registered. If not, we will forward them a registration link.
- The deadline for hotel reservations is today, March 7. For information regarding the hotel name and contact information, please visit the NFCTE website at: https://www.iir.com/Registration/fc.

Anything you can do to assist with these items would be most appreciated, and please let me know what I may do to assist you as well.

Thank you, Diane

Diane G. Ragans
Institute for Intergovernmental Research
(b)(6)

From: Diane Ragans
Sent: Tuesday, March 06, 2012 5:12 PM
To: 'Mabeus, Steven'
Subject: FW: CVE Session at the NFCTE
Importance: High

Hi Steve.

With all the emails you've been receiving from our staff over the past couple days, I expect you know the timelines we are operating under to get the sessions finalized and the presenters confirmed, so I definitely won't hound you about that. You did indicate earlier today that you were supposed to have a meeting with your team working on the session below, so I'm just checking back to determine if anything had been finalized.

I appreciate all of your assistance with this. Thank you, Diane

From: Diane Ragans
Sent: Monday, March 05, 2012 9:13 PM
To: 'Mabeus, Steven'
Subject: CVE Session at the NFCTE
Importance: High

Hi Steve. I hope this message finds you well.

I spoke with Kevin Saupp late this afternoon and he asked me to follow-up with you about this session which will be modified per your comments noted below.

I am the staff POC for this session and if you are available tomorrow, I'd like to give you a call to discuss it further. Realizing our time to finalize the agenda is upon us, I appreciate you being able to work with me at your earliest convenience.

I look forward to speaking with you and working with you on this session. Regards, Diane

Diane G. Ragans
Institute for Intergovernmental Research

(b)(6)

From: Trelles D'Alemberte
Sent: Thursday, March 01, 2012 3:29 PM
To: Diane Ragans
Subject: comments on your Dori Panel

Breakout Session F3

(b)(5)

Summary: The presenters will discuss the Southern Nevada Counter Terrorism Center's (SNCTC's) Partnerships Against Terrorism initiative which revolved around the goal of advancing fusion center counterterrorism and CVE engagement efforts beyond the traditional means and audiences. There were three unique but interconnected pieces that made up the project: 1) translating the See Something Say Something message and making it more community conscious, 2) harnessing the power of social media for countering terrorism and violent extremism, and 3) leveraging non-traditional media outlets to better reach our immigrant communities.

-

Recognizing that the original See Something Say Something message was not sufficiently reaching and resonating with immigrant communities, the message was translated into Arabic, Urdu, Hebrew Amharic, and Spanish; and its image and delivery was modified to become more attractive.

In addition to transforming the message, Counter Terrorism specific Facebook, Twitter, and Youtube accounts were created for the dual purpose of engaging the community and developing sources via the internet. These accounts are used to notify the community of terrorism preventions and awareness information, gauge the community's interests and grievances, and overtly identify and recruit potential sources.

Lastly, pre-existing and new relationships were developed with people in the community that could assist in promoting the message on immigrant-centric media outlets. After some professional source development, the project involved leveraging newspapers, magazines, news channels, and radio stations that were more visible within the immigrant and foreign language speaking communities.

(b)(7)(C)

1. Countering Violent Extremism: Federal, State and local activities and best practices for implementing elements of the White House Strategic Implementation Plan (SIP) for CVE. This panel will an overview of the program and review the actions associated with the plan and the roles and functions of different agencies at the Federal, State and local level.

- • * **Countering Violent Extremism Activity Overview**: The SIP directs Federal Government activity in three specific areas: enhancing engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals.

- • * **Case Studies**: The analysis of select international and domestic terrorism cases have revealed behaviors and indicators associated with indicted and convicted terrorists. These behaviors and indicators while not always associated with violence may be activities that State and local officials and authorities can observe as an individual mobilizes toward violence.

POC: Steve Mabeus
Presenter: FBI, DHS, NCTC and JRIC

Sender: Houser, Jason (b)(6)
Recipient: "Braun, Jacob (b)(6)
"Mabeus, Stev
(b)(6)
"Duggan, Alair
"Saupp, Kevin

"Snyder, Nathaniel (b)(6)
(b)(6)

Sent Date: 2012/03/08 10:11:08

Delivered Date: 2012/03/08 10:11:11

From: Duggan, Alaina (b)(6)
(b)(5)
To: "Saupp, Kevin (b)(5)
(b)(5)
"Snyder, Natha
(b)(5)
CC: "Shoedel, Deborah <(b)(5)
(b)(5)
Subject: RE: FC Panel re: CVE
Date: 2012/03/07 17:32:09
Priority: Normal
Type: Note

Okay – we're going to talk to Steve and the CVE/CT group (John) will take lead getting this pulled together.

From: Saupp, Kevin
Sent: Wednesday, March 07, 2012 5:26 PM
To: Duggan, Alaina; Snyder, Nathaniel
Cc: Shoedel, Deborah
Subject: RE: FC Panel re: CVE

Steve M was working it for us...

From: Duggan, Alaina
Sent: Wednesday, March 07, 2012 5:24 PM
To: Saupp, Kevin; Snyder, Nathaniel
Cc: Shoedel, Deborah
Subject: RE: FC Panel re: CVE

(b)(5)

From: Saupp, Kevin
Sent: Wednesday, March 07, 2012 5:20 PM
To: Duggan, Alaina; Snyder, Nathaniel
Cc: Shoedel, Deborah
Subject: RE: FC Panel re: CVE

We have one: see below draft description–

(b)(5)

(b)(5)

From: Shoedel, Deborah
Sent: Wednesday, March 07, 2012 5:06 PM
To: Saupp, Kevin
Subject: Fw: FC Panel re: CVE

From: Duggan, Alaina
Sent: Wednesday, March 07, 2012 05:03 PM
To: Shoedel, Deborah
Subject: FC Panel re: CVE

Deb,

John Cohen would like to have a panel at the FC Event in Phoenix be focused on CVE. Can you help to make this happen??

Thank you,
Alaina

Sender: Duggan, Alaina <(b)(6)
Recipient: "Saupp, Kevin <
"Snyder, Nathan
(b)(5)
"Shoedel, Debor
(b)(5)
Sent Date: 2012/03/07 17:32:08
Delivered Date: 2012/03/07 17:32:09

2 page draft "CVE Conference at NCTC"

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

2 page draft "DHS/FBI/NSI meeting with ACLU"

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

2 page draft document "SSJ CVE Training update"

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: Saupp, Kevin </(b)(6)
To: (b)(6)
(b)(6)
CC: "Snyder, Nathaniel <(b)(6)
(b)(6)
Subject: RE: TASKING: CVE Work Shop After Action Report REVIEW
Date: 2011/12/06 12:28:11
Priority: Normal
Type: Note

Tim- see attached email to the planning team, as you were on the distro.

-----Original Message-----
From: (b)(6)
Sent: Tuesday, December 06, 2011 11:34 AM
To: Saupp, Kevin
Subject: RE: TASKING: CVE Work Shop After Action Report REVIEW

Kevin-

Can you let me know who was on the CVE Workshop Planning Group? I attend several meeting and helped develop some of the language in the agenda but have never seen this document so I may not have been on the formal planning team but would like to know who was.

(b)(6)

For Official Use Only (Sensitive But Unclassified)/Exempt Predecisional

-----Original Message-----
From: Saupp, Kevin
Sent: Tuesday, December 06, 2011 11:30 AM
To: (b)(6)
Subject: Re: TASKING: CVE Work Shop After Action Report REVIEW

Sure, the full CVE Workshop Planning Group which planned the columbus workshop reviewed it. It has since been handed over to Nate to handle review with the CVE working group, OPA, and the front office.

----- Original Message -----
From: (b)(6)
Sent: Tuesday, December 06, 2011 11:26 AM
To: Saupp, Kevin
Subject: RE: TASKING: CVE Work Shop After Action Report REVIEW

Kevin-

Could you tell me who at DHS has reviewed this document thus far?

(b)(6)

For Official Use Only (Sensitive But Unclassified)/Exempt Predecisional

-----Original Message-----
From: Saupp, Kevin
Sent: Monday, December 05, 2011 4:57 PM
To: (b)(6) Snyder, Nathaniel
Subject: Re: TASKING: CVE Work Shop After Action Report REVIEW

Thanks - we can certainly have them make those changes -

------Original Message------
From (b)(6)
To: Kevin Saupp
To: Snyder, Nathaniel
Cc: Houser, Jason
Cc: Steven Mabeus
Subject: RE: TASKING: CVE Work Shop After Action Report REVIEW
Sent: Dec 5, 2011 4:53 PM

(b)(5)

(b)(6)

For Official Use Only (Sensitive But Unclassified)/Exempt Predecisional
From: Saupp, Kevin Sent: Monday, December 05, 2011 4:41 PM To: Curry, Timothy; Snyder, Nathaniel Cc: Houser, Jason; Mabeus, Steven Subject: RE: TASKING: CVE Work Shop After Action Report REVIEW

(b)(6) - it was put together in a professional publishing program, so we don't have a non-pdf at this point (post the one that was previously sent out to the CVE Workshop working group).

From: (b)(6) Sent: Monday, December 05, 2011 4:27 PM To: Snyder, Nathaniel Cc: Houser, Jason; Mabeus, Steven; Saupp, Kevin Subject: RE: TASKING: CVE Work Shop After Action Report REVIEW

Nate-

Are we getting a non PDF version?

(b)(6)

For Official Use Only (Sensitive But Unclassified)/Exempt Predecisional
From: Snyder, Nathaniel Sent: Friday, December 02, 2011 6:31 PM To: CVE Working Group Cc: Houser, Jason; Mabeus, Steven; Saupp, Kevin Subject: TASKING: CVE Work Shop After Action Report REVIEW

(b)(5)

IGA, CRCL, OPA, I&A, S&T, PLCY and FEMA are required to comment.
Comments are due COB Friday December 9th.

Please work with your CVEWG leads to submit comments (list of CVEWG leads is below).

CVEWG leads or lead designee, please send collected comments to Nathaniel.Snyder(b)(6) nd (b)(6)

Thanks,

-Nate

(b)(7)(C)

(b)(7)(C)

Sender: Saupp, Kevin <(b)(6)

Recipient: (b)(6) (b)(6)
(b)(6)
"Snyder, Nathanie
(b)(6)

Sent Date: 2011/12/06 12:27:54

Delivered Date: 2011/12/06 12:28:11

From: (b)(6)

To:

CC:

(b)(6)

Subject: CVE Workshop - Draft AAR
Date: 2011/10/26 12:30:00
Priority: Normal
Type: Note

CVE Planning Team-

Thank you again for your support in developing and delivering the National Countering Violent Extremism Workshop. Attached to this email is a DRAFT After Action Report (AAR) for the Workshop with a high level summary of the discussions. This AAR was intentionally designed not to attribute specific comments to individuals so that the AAR can be widely shared and posted on the DHS webpage once finalized.

The attached draft document is not for further distribution beyond the planning team, and we would like to request any feedback or comments you may have on the draft AAR by COB November 4, 2011.

Thanks,

Kevin

From: FusionCenterSupport
Sent: Tuesday, August 16, 2011 5:25 PM
To: (b)(6)
(b)(6)
Subject: CVE Workshop - Thank You

CVE Planning Team-

Thank you again for your support in developing and delivering the National Countering Violent Extremism Workshop to meet the needs of our state and local partners. As a result, we successfully achieved our three goals aimed at:

1. Understanding the violent extremism phenomenon in the homeland;
2. Building awareness of the violent extremism threat to local communities; and
3. Supporting fusion centers to develop better intelligence products to support law enforcement customers.

More than 160 state, local, and federal law enforcement participated, including representatives from fusion centers and the largest law enforcement agencies across the country. As a result there was a great synergy among participants and new partnerships were forged. We are currently in the process of developing an after action report with recommendations for next steps, and will share this with you upon completion.

In the meantime, we have posted some additional material on the CVE Workshop Website resources page: http://www.iir.com/registration/cveworkshop/attendees.aspx. The password is (b)(6)
Please do not disseminate the password.

Again, thank you for your time and partnership.

Sender: FusionCenterSupport <(b)(6)
(b)(6)
Recipient: (b)(6)

(b)(6)

Sent Date: 2011/10/26 12:30:22

Delivered Date: 2011/10/26 12:30:00

Page 09 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19 of 23

Withheid pursuant to exemption

(b)(5)

of the Freedom of ınformation and Privacy Act

Page 20 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23 of 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

CVE TALKING POINTS FOR DAS KOUMANS

INTERNATIONAL ACTIVITIES:

- DHS is working in partnership with Europol and EU partners to share best practices, case studies, and information sharing practices regarding CVE.
  - Prior to the G8 Summit in May 2012, the US and EU will share case studies, training curricula, database of internet behaviors and indicators used for violent extremism, and fusion center assessments.

TALKING POINTS:

The White House CVE strategy was released in August 2011. On December 8, 2011, after 5 months of planning and consultation with interagency partners, the White House released the Strategic Implementation Plan (SIP) for the Administration's CVE Strategy.

- The SIP lists the current and future actions the USG will take in support of a locally-focused, community-based approach, in three broad areas:
  - **Enhancing Engagement with and support to local communities:** Our aims in engaging with communities to discuss violent extremism are to (1) share sound, meaningful, and timely information about the threat of radicalization to violence with a wide range of groups and organizations; (2) respond to concerns about government policies and actions; and (3) better understand how we can effectively support community-based solutions.
  - **Building Government and Law Enforcement Expertise:** We are building robust training programs to ensure that communities, government, and law enforcement receive accurate, intelligence-based information about the dynamics of violent extremism. Misinformation about the threat and poor training harms our security by sending stakeholders in the wrong direction and creating tensions with communities.
  - **Countering Violent Extremist Propaganda while Promoting our Ideals:** We will aggressively counter violent extremist ideologies – including on the Internet – by educating and empowering communities and promoting our ideals. In the case of our current priority, we will, through our words and deeds, rebut al-Qa'ida's lie that the United States is somehow at war with Islam.
- The SIP Approach underscores the strength of community-based problem solving, local partnerships, and community-oriented policing. We are building our efforts from existing structures, while creating capacity to fill gaps as we implement programs.

As the activities described in the SIP are executed, there will be major and long-lasting impacts:

- There will be platforms throughout the country for including communities that may be targeted by violent extremists for recruitment and radicalization into ongoing Federal, State and local engagement efforts;
- The Federal Government will support that engagement through a task force of senior officials from across the government;
- Community-led efforts to build resilience to violent extremism will be supported;

- Analysis and production will increase in depth and relevance, and will be shared with those assessed to need it, including Governor-appointed Homeland Security Advisors, Major Cities Mayors' Offices, and local partners;
- Training for Federal, State, tribal, and local government and law enforcement officials on community resilience, countering violent extremism, and cultural competence will improve, and that training will meet rigorous professional standards; and
- Local partners, including government officials and community leaders, will better understand the threat of violent extremism and how they can work together to prevent it.

DHS focuses on working with local authorities and community members.

- We face a threat environment where violent extremism is neither constrained by international borders, nor limited to any single ideology.
- We know that foreign terrorist groups affiliated with al-Qa'ida, and individual terrorist leaders, are actively seeking to recruit Westerners to carry out attacks against U.S. targets.
- We also know that individuals based in the Homeland promote violence inspired by ideological beliefs.
- This is not a phenomenon restricted solely to one community and any effort to counter violent extremism (CVE) must be applicable to all ideologically motivated violence.
- We are a risk-based organization and we prioritize the utilization of resources based on what intelligence and analysis tells us presents the greatest threat to the Homeland.
- At DHS, we believe that local authorities and community members are best able to identify those individuals or groups residing within their communities exhibiting dangerous behaviors—and intervene—before they commit an act of violence.
- Everyone has a role to play in the safety and security of our nation, and time and again we see the advantage of public vigilance and cooperation, from information-sharing, community-oriented policing, and citizen awareness.
- Countering violent extremism is a shared responsibility, and DHS continues to work with a broad range of partners to gain a better understanding of the behaviors, tactics, and other indicators that could point to terrorist activity, and the best ways to mitigate or prevent that activity.
- The Department's efforts to counter violent extremism (CVE) are three-fold, requiring us to:
  - ➢ **Better understand the phenomenon of violent extremism**, and assess the threat it poses to the Nation as a whole, and within specific communities;
  - ➢ **Bolster efforts to address the dynamics of violent extremism** and strengthen relationships with those communities targeted for recruitment by violent extremists; and
  - ➢ **Expand support for information-driven, community-oriented policing efforts** that have proven effective in preventing violent crime across the Nation for decades.

<u>IF ASKED:</u>

What has DHS done to work across the homeland security enterprise to counter violent extremism and other threats?

- The Department has worked with state, local and tribal governments across the nation to incorporate homeland security and terrorism prevention efforts into day-to-day efforts to protect our communities from violent crime. These efforts include:

- Establishing robust information sharing capabilities to provide state, local, and private sector authorities credible and specific, CLASSIFED and UNCLASSIFIED, threat-related information;
- Building analytic capacity at the grass-roots level by supporting regional fusion centers so that national intelligence can be viewed within the context of local conditions thereby allowing state, local and tribal authorities to better assess the risk to their communities;
- Providing frontline personnel with Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) training as to the behaviors and indicators associated with specific threats and terrorism-related crime so that our 800,000 state, local and tribal officers can better recognize terrorism-related suspicious activities; and
- Raising public awareness to the behaviors and indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities., for example the Department's nationwide launch of the "If You See Something, Say Something ™" campaign.

How has the Department's CVE strategy aided in recent terrorist plots?

- If something is wrong, somebody locally will probably become aware. Our challenge is connecting those individuals with an appropriate response.
- A study from 2010 found that, between 1999 and 2009, more than 80 percent of foiled terrorist plots in the United States were thwarted because of observations from law enforcement or the general public.
- An examination of 86 terrorist cases in the U.S. from 1999 to 2009 by the Institute for Homeland Security Solutions shows that nearly half of those cases were related to al-Qaeda or al-Qaeda-inspired ideology, with the remainder due to a number of other violent extremist motivations
- By promoting public vigilance and community-policing efforts we are expanding our information sharing capabilities beyond local law enforcement, and by reporting suspicious behaviors we are able to intervene before there is an act of violence.

What is DHS doing to combat violent extremism?

- DHS CVE efforts include law enforcement training, community engagement, grievance resolution and enhanced efforts to understand the issue of violent extremism through S&T research and I&A analysis. These efforts are coordinated with the inter-agency and the NSS.
- DHS is expanding its support for local, information-driven community-oriented efforts to prevent violent crime and build safe, secure and resilient communities.
- Local community/government partnerships represent the best opportunity to identify and mitigate violence that may be ideologically motivated.

How is the federal government engaging frontline officers and community partners on countering violent extremism?

- Through our Office for Civil Rights and Civil Liberties (CRCL), DHS continues to educate tribal, state and local law enforcement on cultural awareness and how best to engage with communities.
- To date, CRCL has already trained more than 2,490 police officers on ways to counter violent extremism in their own communities.
- DHS and the Department of Justice have also trained over 166,000 frontline officers through the Nationwide Suspicious Activity Reporting (SAR) Initiative and hope to reach all of America's officers on the frontlines by fall of 2011.

- In addition to these training initiatives, DOJ and DHS, under the Building Communities of Trust Guidance, have coordinated engage our state and local law enforcement and community partners to share best practices on forming working partnerships and community based solutions in meetings across the country.
- DHS is working with state, local, tribal and federal partners to develop a CVE Curriculum for state, local, tribal, and federal law enforcement as well for use at academics.

From: (b)(6) (b)(5)
(b)(5)
To: "Saupp, Kevin (b)(5)
(b)(5)
"Snyder, Natha
(b)(5)
CC: "Houser, Jason < (b)(5)
(b)(5)
"Mabeus, Steven
(b)(5)
Subject: RE: TASKING: CVE Work Shop After Action Report REVIEW
Date: 2011/12/05 16:53:56
Priority: Normal
Type: Note

Given that how do you want the edits provided. There are some changes that will need to be made with the obvious one being that the three objectives listed as the core of the NSS CVE Strategy are not the same ones in the WH document and use different language which is problematic.

Here are the three as copied and cut from the NSS Document:

(b)(5)

(b)(6)

For Official Use Only (Sensitive But Unclassified)/Exempt Predecisional

From: Saupp, Kevin
Sent: Monday, December 05, 2011 4:41 PM
To: (b)(6) Snyder, Nathaniel
Cc: Houser, Jason; Mabeus, Steven
Subject: RE: TASKING: CVE Work Shop After Action Report REVIEW

Tim – it was put together in a professional publishing program, so we don't have a non-pdf at this point (post the one that was previously sent out to the CVE Workshop working group).

From: (b)(6)
Sent: Monday, December 05, 2011 4:27 PM
To: Snyder, Nathaniel
Cc: Houser, Jason; Mabeus, Steven; Saupp, Kevin
Subject: RE: TASKING: CVE Work Shop After Action Report REVIEW

Nate-

Are we getting a non PDF version?

(b)(6)

For Official Use Only (Sensitive But Unclassified)/Exempt Predecisional

From: Snyder, Nathaniel
Sent: Friday, December 02, 2011 6:31 PM
To: CVE Working Group
Cc: Houser, Jason; Mabeus, Steven; Saupp, Kevin
Subject: TASKING: CVE Work Shop After Action Report REVIEW

(b)(5)

-Nate

TSA (b)(7)(C)

CBP	(b)(7)(C)
ICE	
USCIS	
USSS	
FEMA	
USCG	
NPPD	
CRCL	
IGA	
OPA	
I&A	
OPS	
PLCY/CT	
FLETC	
OGC	
OLA	
SEC	
S2	
PRIV	
S&T	

Sender: Curry, Timothy (b)(5)
Recipient: "Saupp, Kevin <

"Snyder, Nathaniel (b)(6)
(b)(5)
"Houser, Jason </
"Mabeus, 5teven <

Sent Date: 2011/12/05 16:53:55
Delivered Date: 2011/12/05 16:53:56

4 page draft "CVE TP's for DAS Koumans" final released in full

Page 1 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 4 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

10 page draft "Communication plan for SIP DHS and NCTC"

Page 01 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

10 page draft "communication plan for SIP V1"

Page 01 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

10 page draft "communication plan for SIP v1"

Page 01 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

24 page draft "SIP"

Page 01 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of ınformation and Privacy Act

Page 07 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

24 page draft "SIP"

Page 01 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE CHARLES E. GRASSLEY

Secretary Janet Napolitano
Oversight of the Department of Homeland Security
October 19, 2011

Threat of Islamic Terrorism

Question 1: Your written testimony was frustratingly vague about the terrorist threat the United States faces. You briefly mentioned the continuing threat from al-Qaeda and its affiliates, but for most of your discussion of the terrorist threat, you referred only to undifferentiated "terrorism" or "violent extremism."

In its Final Report, the National Commission on Terrorist Attacks Upon the United States (the "9-11 Commission"), stated, "[T]he enemy is not just 'terrorism,' some generic evil. This vagueness blurs [counter-terrorism] strategy. The catastrophic threat at this moment in history is more specific. It is the threat posed by Islamist terrorism—especially the al-Qaeda networks, its affiliates, and its ideology." (emphasis in the original.)

Do you agree with the 9-11 Commission that, "The catastrophic threat at this moment in history …is the threat posed by Islamist terrorism?"

ANSWER: **Yes.** The Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) assesses that the most significant terrorist threat to the homeland is that posed by al-Qa'ida, its affiliates and allies, and homegrown violent extremists (HVEs) inspired by al-Qa'ida's ideology. This long term threat stems from the violent, anti-Western nature of al-Qa'ida's ideology, and individuals who adhere to this belief system as justification for violent action.

Do you agree with the 9-11 Commission that the "ideology" of al-Qaeda is a threat and must be countered?

Yes. Al-Qa'ida's narrative of hatred and violent opposition to democracy, the West, and non-Muslims in general represents a threat to the United States and its allies but it also represents a threat to achieving peace and stability in the Middle East and South Asia. Al-Qa'ida opposes democratic institutions that are essential to the development of good governance and its advocacy of violence to further its goals undermines the stability of countries it targets.

How would you define the "ideology" of al-Qaeda?

Al-Qa'ida's ideology is best described using its own words, as detailed in Usama bin Ladin's 1998 fatwa: "…to kill Americans and their allies—civilian and military—is an individual duty of every Muslim who can do it in any country in which it is possible to do it." These directives extend also to efforts to exploit the resources of the United States, as bin Ladin further asked followers to "…comply with God's order to kill the Americans and plunder their money wherever and whenever they find it." DHS is most concerned about individuals who use this ideology and premise to conduct acts of violence.

Threat of Homegrown Violent Extremism

Question 2: In your written testimony, you note "a conscious effort by terrorists to recruit people who are already in the United States" and refer to this as the "threat of homegrown violent extremism."

What is your definition of "homegrown violent extremism"?

ANSWER: DHS and the Federal Bureau of Investigation (FBI) define a HVE as a person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically-motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization, but is acting independently of direction by a foreign terrorist organization. HVEs are distinct from traditional domestic terrorists who engage in unlawful acts of violence to intimidate civilian populations or attempt to influence domestic policy without direction from or influence from a foreign actor.

Please give examples of major attempted or successful terrorist attacks conducted by homegrown violent extremists.

The threat from HVEs appears to be growing. The Congressional Research Service reported in September 2010 that 19 arrests of HVEs were made between May 2009 and August 2010, compared to 21 such plots in the entire period between September 11, 2001 and May 2009. The Heritage Foundation reported in a May 2011 report that 39 plots involving HVEs had been disrupted since the September 11, 2001 attacks. Most plots are disrupted before they can occur through effective work by the FBI and its Joint Terrorism Task Forces. Examples of some recent disrupted plots include:

- The arrest of Naser Abdo$^{\text{USPER}}$ in June 2011 for allegedly plotting to attack Ft. Hood, Texas.

- The arrest by the New York Police Department in May 2011 of Mohamed Mamdouh$^{\text{USPER}}$ and Ahmed Ferhani after they attempted to purchase a hand grenade, guns, and ammunition to attack an unidentified synagogue.

- Mohamed Osman Mohamud's$^{\text{USPER}}$ November 2010 alleged failed attempt to bomb a Christmas celebration in Portland, Oregon.

- The arrest of Farooque Ahmed$^{\text{USPER}}$ in October 2010 for allegedly plotting to attack the Washington, DC subway system.

In addition to disrupted plots, 2009 saw two fatal attacks with the Ft. Hood shootings allegedly carried out by Nidal Hasan$^{\text{USPER}}$ and the shooting of two military recruiters in Little Rock, Arkansas by Carlos Bledsoe$^{\text{USPER}}$.

Which terrorist groups are trying to recruit people in the United States?

Al-Qa'ida, its affiliates, and groups ideologically aligned with them have attempted to inspire persons based in the United States to support their operations. Any terrorist group that can benefit from fundraising, acquisition of material, or recruiting activities in the United States is likely to attempt to recruit people in the United States.

Foreign terrorist groups affiliated with al-Qa'ida and individual terrorist thought leaders who ascribe to al-Qa'ida's ideology actively seek to inspire Westerners to carry out attacks against Western and United States targets. These parties seek to inspire individuals living in communities within the United States via print, video, and social media, as well as through personal interaction.

This is not a phenomenon restricted solely to one community. The threat posed by violent extremists is real and not limited to a single ideology. Individuals inspired by the sovereign citizen extremist movement, white supremacist extremist movement, militia extremist movement, anti-abortion extremist movement, animal rights extremist movement, and the anarchist extremist movement have attempted to or carried out acts of violence in the US over the past few years. The threat environment constantly evolves, which is why DHS must consider all types of violent extremism.

With what methods and arguments are they trying to recruit people?

Al-Qa'ida and its affiliates increasingly have relied on Western ideologues—particularly American citizens like the now-deceased Anwar al-Aulaqi and Samir Khan, as well as Omar Hammami$^{\text{USPER}}$, and Adam Gadahn$^{\text{USPER}}$ to convey their message via increasingly sophisticated English-language propaganda. The increasing availability on the Internet of materials advocating attacks against the United States and providing practical operational advice, combined with social networking tools that facilitate violent extremist communication, has contributed to a more diversified and challenging threat picture in the United States. Due in part to these factors, propaganda releases by even deceased ideologues such as al-Aulaqi have the potential to remain transcendent and inspire violent action by individuals within the United States.

- Al-Aulaqi, Khan, and Hammami have appealled to potential violent extremists through their use of colloquial English, slick presentations and the use of social networking sites such as YouTube^{USPER} and Facebook^{USPER}.

- These violent extremist ideologues—al-Aulaqi and Khan in particular—spearheaded recent efforts to provide Americans and other Westerners with the ability to independently plan and execute their own terrorist attacks without the need to travel overseas for training—through English-language propaganda.

Whom are they trying to recruit—American citizens, legal permanent residents, refugees, illegal aliens, all of the above?

Al-Qa'ida, its affiliates, and likeminded groups attempt to inspire anyone who has access to the United States and can further their operations. Al-Qa'ida and al-Qa'ida in the Arabian Peninsula have focused recent propaganda on Western, English-speaking Muslims, and their messages have resonated and inspired some people to carry out or plot acts of violence, including US-born and naturalized citizens and Legal Permanent Residents. A few examples include:

- Others have been inspired by al-Qa`ida's message to carry out attacks on their own. Alleged November 2009 Ft. Hood shooter Nidal Hasan, Carlos Bledsoe who shot two serviceman at a recruiting center in Arkansas in 2009, and Michael Finton,^{USPER} who plotted to blow up a court house in Springfield, Illinois are examples of lone offenders inspired by violent extremist propaganda.

Community Efforts to Counter Violent Extremism

Question 3: In your written testimony, you state that "law enforcement officials work with members of diverse communities that broadly and strongly reject violent extremism."

Please specify which communities you were referring to.

ANSWER: The Administration's and DHS' approach to countering violent extremism (CVE) emphasizes the strength of local communities. Local communities are best placed to recognize the threat and push back against violent extremists who may be targeting their families and neighbors. Our Nation's homeland security is based on the premise that we must harness local efforts to counter national threats. DHS is contributing to multiple interagency efforts, and with non-federal and non-governmental partners, to engage local communities in our CVE efforts to make them safe, secure, and resilient. Our understanding of why an individual becomes a violent extremist continues to mature, and we continue to work with communities to better understand the dynamics that may contribute to that outcome.

- Through our Office for Civil Rights and Civil Liberties (CRCL), DHS continues to educate tribal, state and local law enforcement on cultural awareness and how best to engage with communities.
- CRCL doubled its outreach to communities this year and expanded quarterly engagement roundtables to 14 cities throughout the country. During FY2011, CRCL also conducted 72 community engagement events with communities including those based on CVE- related topics
- To date, CRCL has also trained more than 2,490 police officers on ways to counter violent extremism in their own communities.
- DHS and the Department of Justice have also trained over 180,000 frontline officers through the Nationwide Suspicious Activity Reporting (SAR) Initiative and hope to reach all of America's officers on the frontlines by fall of 2011.
- In addition to these training initiatives, DOJ and DHS, under the Building Communities of Trust Guidance, have coordinated engage our state and local law enforcement and community partners to share best practices on forming working partnerships and community based solutions in meetings across the country.
- DHS is working with state, local, tribal and federal partners to develop a CVE Curriculum for state, local, tribal, and federal law enforcement as well for use at academies.

We are expanding outreach to communities that may be targeted for recruitment by violent extremists; engaging those communities on issues of common interest; promoting greater awareness and understanding of Federal resources, programs, and security measures; and addressing community concerns.

DHS continues to work closely with state and local partners, and individual citizens, to raise awareness through initiatives such as the "If You See Something, Say Something™" public awareness campaign and the Nationwide Suspicious Activity Reporting (SAR) Initiative. The See Something/Say Something campaign provides all citizens a positive role in securing our country. The SAR initiative, meanwhile, leverages the power of state and local first responders to identify potential terrorist activity, providing law enforcement the opportunity to disrupt and dismantle terrorist plots. The SAR Initiative provides a standardized system for reporting suspicious activity based on behavior analyzed across national trends and shared across jurisdictions and sectors. In many cases, information shared through the SAR Initiative provides a medium for sharing valuable information across the Intelligence Community that previously went unharvested and unevaluated.

Please rank in order of threat, from highest to lowest, the types of violent extremism (e.g., violent Islamic extremism, environmental/animal rights activists, militias, white supremacist movements, etc.) that the United States faces.

- We face a threat environment where violent extremism is neither constrained by international borders, nor limited to any single ideology.

- We know that foreign terrorist groups affiliated with al-Qa'ida, and individual terrorist leaders, are actively seeking to recruit Westerners to carry out attacks against U.S. targets.

- We also know that individuals based in the Homeland promote violence inspired by ideological beliefs.

- This is not a phenomenon restricted solely to one community and any effort to counter violent extremism (CVE) must be applicable to all ideologically motivated violence.

At present, we judge that threats from al-Qa'ida and its affiliates pose the greatest threat to the homeland. These groups have demonstrated great persistence, resilience, and capability in plotting to carry out attacks against the United States despite a series of setbacks. Their recent encouragement of individual action by their supporters complicates the threat picture, as individuals acting in support of their ideology may not be in contact with overseas plotters and thus may escape notice of the Intelligence Community. Individuals exploiting information on explosives and terrorist tactics on the Internet potentially can carry out attacks with compressed time for training and planning.

The threat of violence from domestic violent extremists also emanates from small, clandestine cells or individuals acting independently. In just the past three years, there have been several incidents involving domestic extremists committing or attempting violent acts. For example, lone offenders from the white supremacist extremist movement attacked a guard at the U.S. Holocaust Museum in Washington, DC in 2009 and attempted to bomb a Martin Luther King, Jr. Day parade in Washington State in 2011, while a lone anti-abortion extremist in Kansas murdered an abortion doctor in 2009. In 2010, two unaffiliated sovereign citizen extremists murdered two law enforcement officers in Arkansas during a traffic stop, while several other unaffiliated sovereign citizen extremists have attempted to kill law enforcement officers. Lastly, animal rights extremist activity in the Homeland seems to be on the increase. A self-proclaimed animal rights extremist in Utah was arrested and pled guilty to burning down a leather factory, and restaurant, and a Colorado sheepskin factory in 2011. Consequently, our analysis focuses on the possible tactics and targets of these cells or individuals, as well as violent extremist groups.

I&A Resources

Question 4: ***Please describe how the resources of DHS, in particular the Office of Intelligence and Analysis and the rest of the DHS Intelligence Enterprise are allocated in accordance with your ranking of priorities.***

ANSWER: I&A and the rest of the DHS Intelligence Enterprise do not allocate intelligence resources exclusively to one particular terrorist group or movement.

We remain mindful that al-Qa'ida, its affiliated and allied groups, and those motivated by its ideology, remain the primary focus of DHS analytic efforts. Additionally, analysts within DHS focus on a variety of related topics and issues, to include homegrown violent extremism; terrorist tactics, techniques, and procedures; terrorist travel and immigration security; chemical and biological weapons use or development by terrorist groups; as well as violent domestic terrorist groups. We partner with the DHS Intelligence Enterprise in every way possible to gain valuable insight and added-value on these subjects, using CBP data and reporting to inform our analysis on terrorist travel, as well as information from the state and local fusion centers on homegrown violent extremism and domestic terrorism. Finally, our Intelligence Community partners remain a vital source of partnership, as information provided by FBI and NCTC in particular assists our understanding of developing threats that may require sharing with our state and local partners.

8 page draft "Questions for the record submitted by The Honorable Charles E. Grassley"

Page 1 of 8

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 8

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 8

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 4 of 8

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 5 of 8

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 6 of 8

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 7 of 8

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 8 of 8

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

7 page draft "Questions for the record submitted by The Honorable Charles E. Grassley"

Page 1 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 4 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 5 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 6 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 7 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

25 page draft "SIP"

Page 01 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 25 of 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: (b)(6), (b)(7)c
Subject: (U/ Law Enforcement Resources
Date: Thursday, April 7, 2016 7:10:45 AM
Attachments: oslle-resource-catalog-volumeiv-2-24-2016_1.pdf
image001.gif

From: NOC.SWO.Restricted
Sent: Thursday, April 07, 2016 6:18:20 AM
To: NOC.State&Local; NOC.SWO
Cc: NOC.SWO.Restricted
Subject: (U/ Law Enforcement Resources
Auto forwarded by a Rule

UNCLASSIFIED / FOR OFFICIAL USE ONLY

FYI

https://www.dhs.gov/sites/default/files/publications/oslle-resource-catalog-volumeiv-2-24-2016_1.pdf

DHS National Operations Center (NOC)
Washington, DC//202.282.8101

WARNING: *This document is FOR OFFICIAL USE ONLY (FOUO); it contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552) It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official.*

DHS State and Local Law Enforcement Resource Catalog

Volume IV

February 2016

Intentional Blank Page. Please Continue to Next Page.

Letter from the Office for State and Local Law Enforcement

March 1, 2016

Dear Law Enforcement Partners:

Homeland security begins with hometown security, and DHS tirelessly works to get tools, information, and resources out of Washington, D.C. and into the hands of our state, local, and tribal law enforcement partners. With the release of the *DHS State and Local Law Enforcement Resource Catalog Volume III*, we are pleased to announce a continuation of that effort.

The *DHS State and Local Law Enforcement Resource Catalog* is a one-stop shop for non-federal law enforcement. This document summarizes and provides links to training, publications, newsletters, programs, and services available from across the Department to our law enforcement partners.

At DHS, we are continually developing new programs and resources that could be of assistance to state, local, and tribal law enforcement. If you cannot find what you are searching for in this catalog, please do not hesitate to contact the Office for State and Local Law Enforcement for additional assistance.

The Office for State and Local Law Enforcement has always worked to enhance the support that DHS provides to our law enforcement partners. We hope this catalog is another one of those tools that will assist in your efforts to keep our communities safe, secure, and resilient.

Sincerely,

Office for State and Local Law Enforcement
Department of Homeland Security

Office for State and Local Law Enforcement

Overview

On the recommendation of the 9/11 Commission, Congress created the Office for State and Local Law Enforcement (OSLLE) in 2007 to lead the coordination of DHS-wide policies related to state, local, tribal, and territorial law enforcement's role in preventing, preparing for, protecting against, and responding to natural disasters, acts of terrorism, and other man-made disasters within the United States.

Contact OSLLE

Phone: 202-282-9545

Email: OSLLE@hq.dhs.gov

Website: http://www.dhs.gov/office-state-and-local-law-enforcement-oslle

Responsibilities

- Serve as the primary Department liaison to state, local, tribal, and territorial law enforcement;
- Advise the Secretary on the issues, concerns, and recommendations of state, local, tribal, and territorial law enforcement;
- Keep the law enforcement community informed about Department-wide activities and initiatives such as "If You See Something, Say Something™", the Blue Campaign, Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), and the Department's efforts in Countering Violent Extremism;
- Identify and respond to law enforcement challenges that affect homeland security;
- Coordinate with the Office of Intelligence and Analysis to ensure timely coordination and distribution of intelligence and strategic information to state, local, tribal, and territorial law enforcement; and
- Work with the Federal Emergency Management Agency to ensure that law enforcement and terrorism-focused grants to state, local, tribal, and territorial law enforcement agencies are appropriately focused on terrorism prevention activities.

Helping to Build a Safe, Secure, and Resilient Nation

3/1/16

Table of Contents

Department-Wide Resources

Active Shooter Preparedness Resources. The Department of Homeland Security offers a number of resources to state and local law enforcement for responding to active shooter incidents.

Active Shooter Preparedness resources include a desk reference guide; a poster; and a pocket-size reference card to address how employees, managers, training staff, and human resources personnel can mitigate the risk of, and appropriately react in the event of an active shooter situation. To access all of these resources, visit www.dhs.gov/active-shooter-preparedness. Materials are also available in Spanish.

The Federal Law Enforcement Training Centers (FLETC) offer tuition-free or low-cost training courses, including an Active Shooter Threat Training Portfolio that includes the following training programs:

- *Active Shooter Threat Training Program (ASTTP)* – covers fundalmental/basic skills;
- *Active Shooter Threat Instructor Training Program (ASTITP)* – instructor level, "train-the-trainor" program;
- *Basic Tactical Medical Training Program (BTMTP)* – provide skills to enhance the law enforcement officer's ability to provide emergency first aid for traumatic and non-traumatic injuries during an active threat scenario; and
- *Tactical Medical First Responder (8 hour) Training Program (TMFR)*.

These training programs are designed to provide law enforcement officers with the threat awareness, analytical knowledge, tactical skills, and emergency first aid skills which are needed to successfully serve as a law enforcement first responder in an active shooter/threat situation. They are conducted at selected venues throughout the country, hosted by a local law enforcement agency or at one of FLETC's training delivery points which are located in Artesia, NM; Charleston, SC; Cheltenham, MD; and Glynco, GA. To learn more about FLETC training courses available to state, local, and tribal law enforcement and for contact information, visit https://www.fletc.gov/state-local-tribal or contact stateandlocaltraining@dhs.gov.

Within the Homeland Security Information Network (HSIN), the Joint DHS and FBI Countering Violent Extremism (CVE) and Active Shooter Web Portal provides a forum to share Unclassified For Official Use Only (FOUO), Sensitive but Unclassified (SBU), and Law Enforcement Sensitive (LES) Information with anyone who is a sworn, full-time, salaried, Law Enforcement Officer (Federal, State, or Local); Federal Employee affiliated with the criminal justice system or intelligence communities; military personnel; and governmental agencies associated with infrastructure protection of the United States. The Portal also shares Unclassified FOUO or SBU information with private sector partners, civilian security personnel, corporate executives, academic institution employees, first responders (including firemen and EMS), international partners, religious leaders, and other state and local partners that are not law enforcement personnel, as appropriate. The portal provides users and training practitioners with accurate, appropriate, and relevant CVE and Active Shooter training development resources, subject matter expert information, and outreach initiatives. It also has forums to provide feedback, products useful to others, and allows participants to ask questions concerning CVE or the Active Shooter Program. Persons with a job-related duty, public service interest, or who support a CVE and/or Active Shooter program can request access into this Portal. Work-related information is needed to ensure members are provided the appropriate accesses and their work activities justify a need to know. This information is used to nominate the user into HSIN. The user will then receive an email to validate their information. To request access, email: cveasportal@hq.dhs.gov. Provide the following information in the body of the email:

1. Full Name;
2. Place of Employment;
3. Job Title;
4. Work Email Address;
5. Work Phone Number;
6. Short Job Description as it Relates to CVE or Active Shooter.

Blue Campaign to Fight Human Trafficking. DHS is responsible for investigating human trafficking, arresting traffickers, and protecting victims. The Department also provides immigration relief to victims of human trafficking. The Blue Campaign is the unified voice for the DHS' efforts to combat human trafficking. Working in collaboration with law enforcement, government, non-governmental, and private organizations, the Blue Campaign strives to protect the basic right of freedom and to bring those who exploit human lives to justice. Increased awareness and training will lead to more tips to law enforcement, which results in more victims being identified. We cannot do this alone so please join us in the fight to end human trafficking. Visit the Blue Campaign website to learn about how we can work together and to find out about available training, outreach materials, and victim assistance. To learn more, visit www.dhs.gov/bluecampaign or, contact BlueCampaign@hq.dhs.gov.

You can also report tips to the ICE Tip line at 866-DHS-2-ICE, or 866-347-2423.

Specific Blue Campaign training products include:

- Web-based training about the indicators of human trafficking;
- Roll call videos explaining how available immigration relief for foreign victims provide a benefit to law enforcement;
- Scenario based videos depicting indicators of sex trafficking and labor trafficking;
- Printed educational and reference materials for law enforcement, non-governmental organizations, judicial officials, first responders, school staff, and victims or potential victims; and
- Human trafficking awareness posters and public service announcements.

To access these and other products, visit www.dhs.gov/bluecampaign.

Common Operating Picture (COP) is a suite of capabilities that provides government and private sector Homeland Security Enterprise professionals with enhanced situational awareness to facilitate timely decision support prior to or in the aftermath of a natural disaster, act of terrorism, or man-made disaster. The DHS COP architecture coupled with data from Homeland Security partners and Homeland Security Information Network (HSIN), provides actionable information, enhanced contextual understanding, and geospatial awareness. This enables government and private sector leaders to make timely and informed decisions, and identify courses of action during an event or threat situation. The DHS COP provides users a broad set of capabilities based on best-in-class technologies that deliver a rich, end user experience through a web-accessible interface.

The DHS COP is an application that supports the DHS mission of responding to threats and hazards to the nation by collecting, sharing, and displaying multi-dimensional information that facilitates collaborative planning and responses to these threats. For more information, contact GMO@hq.dhs.gov.

Homeland Security Information Network (HSIN) is a national secure and trusted web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission. Using a single login credential, HSIN provides secure access from multiple networks such as LEEP, RISSnet, Intelink, and

Tripwire. HSIN is made up of growing network of communities, called Communities of Interest (COI). COIs are organized by state organizations, federal organizations, or mission areas such as emergency management, law enforcement, critical sectors, and intelligence. Users can securely share within their communities or reach out to other communities as needed. HSIN provides secure, real-time collaboration tools, including a virtual meeting space, instant messaging, and document sharing. HSIN allows partners to work together instantly, regardless of their location, to communicate, collaborate, and coordinate. This enables government and private sector leaders to make timely and informed decisions, and identify courses of action during an event or threat situation. For more information, visit www.dhs.gov/HSIN.

"If You See Something, Say Something™". The nationwide "If You See Something, Say Something™" public awareness campaign is a simple and effective program to raise public awareness of indicators of terrorism and terrorism-related crime, and to emphasize the importance of reporting suspicious activity to the proper local law enforcement authorities. The campaign was originally used by New York's Metropolitan Transportation Authority, which has licensed the use of the slogan to DHS for anti-terrorism and anti-terrorism crime related efforts. For more information about the initiative, visit www.dhs.gov/ifyouseesomethingsaysomething.

National Terrorism Advisory System (NTAS) has replaced the Homeland Security Advisory System as our nation's primary domestic terrorism alerting resource. This system more effectively communicates information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector. It recognizes that Americans all share responsibility for the nation's security, and should always be aware of the heightened risk of terrorist attack in the U.S. and what they should do. After reviewing the available information, the Secretary of Homeland Security will decide, in coordination with other federal entities, whether an NTAS Alert should be issued. For more information, visit www.dhs.gov/national-terrorism-advisory-system.

U.S. Citizenship and Immigration Services (USCIS)

USCIS is the government agency that oversees lawful immigration to the United States. USCIS will secure America's promise as a nation of immigrants by providing accurate and useful information to our customers, granting immigration and citizenship benefits, promoting an awareness and understanding of citizenship, and ensuring the integrity of our immigration system. Read the full mission statement at www.uscis.gov/aboutus.

Avoid Scams is a webpage for the public to find information about how to recognize and report immigration scams and the unauthorized practice of immigration law, and how to find authorized help with immigration services. To learn more, visit www.uscis.gov/avoidscams, or www.uscis.gov/eviteestafas in Spanish.

Fraud Detection and National Security (FDNS) Units. USCIS Field Operations Directorate FDNS Units are staffed with immigration officers, who are well-versed in immigration related fraud and national security issues. Immigration officers not only assist in the adjudications of immigration benefit applications, but also support programs sponsored by law enforcement agencies, such as Joint Terrorism Task Forces (JTTFs), Document and Benefit Fraud Task Forces (DBFTFs), and state and local fusion centers. Immigraiton officers participation in these programs may be full-time, part-time, or virtual support. Immigration officers conduct administrative site visits and provide general or case-specific immigration information to law enforcement agencies under DHS guidance. Currently there are more than 60 immigration officers in the JTTF Program, and 25 immigraiton officers in most of the 21 ICE-led DBFTFs. In addition, designated immigration officers in all 26 District Offices have made positive contact with a point-of-contact at state and local fusio ncenters, usually the DHS I&A representative. For more information, please contact USCISFODFDNSOps@uscis.dhs.gov.

Law Enforcement Support Operation Unit. USCIS's Fraud Detection and National Security (FDNS) Directorate has developed a centralized operation to administer the S Visa Program and facilitate the issuance of notional ("cover") immigration documents.

The S visa program is available for aliens who possess "critical reliable information concerning a criminal organization or enterprise," who are willing to share or have shared their information with a U.S. law enforcement agency or court and whose presence in the U.S. is necessary for the successful prosecution of criminal activity. The S-6 visa is available to aliens possessing "critical reliable information" regarding terrorist activity. State and federal law enforcement authorities (including federal or state courts and U.S. attorneys) can initiate a request under the "S" category. Requests for "S" status are processed through the requesting agency, the Department of Justice, and ultimately USCIS FDNS.

Notional immigration documents are genuine immigration documents issued to individuals who do not possess the associated immigration status. These documents are issued in furtherance of law enforcement investigations in order to create the appearance that an individual possesses or has been approved for a particular immigration status. Law enforcement requests for notional documents are submitted to U.S. Immigration and Customs Enforcement (ICE), which reviews the notional document request to ensure that documents are being requested for a legitimate investigative purpose. If ICE believes the document request is appropriate, USCIS will consider production of the requested document. For more information, visit http://www.uscis.gov/green-card/other-ways-get-green-card/green-card-informant-s-nonimmigrant.

USCIS's Public Engagement Division (PED) seeks to focus on open, candid, and constructive collaboration with community stakeholders at all levels. PED is dedicated to coordinating and directing agency-wide dialogue with external stakeholders to actively collaborate and maintain open and transparent communication and to seek feedback regarding policies, priorities, and organizational performance reviews. For more information, visit www.uscis.gov or contact Public.Engagement@dhs.gov.

USCIS Resources is a webpage with links to a variety of publications and other materials for USCIS customers, the organizations that serve them, and the public. Visit www.uscis.gov/resources.

USCIS provides the latest version of its applications and petitions on its website. All forms are free and available at www.uscis.gov/forms. For more information, contact Public.Engagement@dhs.gov.

T and U Nonimmigrant Status ("T Visas" and "U Visas") for Victims of Human Trafficking and Other Qualifying Crimes. The T visa is generally available for victims of human trafficking who have complied with any reasonable request for assistance in the investigation or prosecution of the human trafficking, and who meet other requirements. The U visa is generally available for victims of certain qualifying crimes who have been, are being, or are likely to be helpful to law enforcement in the investigation or prosecution of the crime, and who meet other requirements. Federal, state, local, tribal or territorial law enforcement agencies may sign a law enforcement certification for the victim detailing the crime and the victim's cooperation in the investigation or prosecution. U visa petitioners are required to submit this law enforcement certification with their Form I-918, Petition for U Nonimmigrant Status, and T visa applicants may submit a law enforcement certification with their Form I-914, Application for T Nonimmigrant Status. The investigating or prosecuting law enforcement agency does not apply to USCIS for a T or U visa on the victim's behalf. The victim applies to USCIS T and U visa and USCIS reviews the request and all submitted evidence to determine eligibility. Related resources include:

- The **U and T Visa Law Enforcement Resource Guide** provides law enforcement officials information about U and T visa requirements, the law enforcement certification process, and answers to frequently asked questions from law enforcement agencies to support investigations and prosecutions involving immigrant victims of human trafficking and other crimes. Included in the guide is a selection of best practices and a frequently asked questions section that draws upon questions received by state and local law enforcement. The guide is available electronically at http://www.dhs.gov/publication/u-visa-law-enforcement-certification-resource-guide.

- **Information for Law Enforcement Agencies and Judges.** USCIS has a webpage for law enforcement agencies and judges that explains the different types of benefits available for victims of human trafficking and other crimes. It also describes procedures for law enforcement, including a list of "Important Things to Remember." Other materials include roll call videos, information about continued presence (a temporary immigration status administered by ICE for victims of human trafficking), and links to the T visa declaration form and U visa certification form. Both of these forms are completed by the investigating or prosecuting agency but submitted to USCIS by the victim. For more information, visit www.uscis.gov/tools/resources/information-law-enforcement-agencies-and-judges. For law enforcement inquiries, contact LawEnforcement_UTVAWA.vsc@uscis.dhs.gov.

- **In-Person and Web-Based Training**. USCIS offers in person and web-based presentations for law enforcement on T and U visas. If interested, contact USCIS at T_U_VAWATraining@uscis.dhs.gov.

Citizenship and Immigration Services Ombudsman (Ombudsman's Office)

The Ombudsman's Office is available to help law enforcement with issues or concerns that they have regarding their interactions with USCIS. The Ombudsman's Office is an independent, impartial, and confidential office within DHS that helps individuals and employers resolve problems with USCIS applications and petitions. The office also makes recommendations to fix systemic problems and improve the overall delivery of services provided by USCIS.

Send Your Recommendations to the Ombudsman's Office. The Ombudsman is dedicated to identifying systemic issues in the immigration benefits process and preparing recommendations for submission to USCIS for process changes. Send examples of identified issues and suggestions to cisombudsman@hq.dhs.gov.

Submit a Request for Case Assistance to the Ombudsman's Office. If you, or someone you are working with, are experiencing problems during the adjudication of an immigration benefit with USCIS, you can submit an electronic DHS Form 7001 through the Ombudsman Online Case Assistance system. To submit a request for assistance on behalf of another, follow the form instructions to ensure the appropriate party consents to your submission of the request for assistance. For more information, see www.dhs.gov/case-assistance.

Office for Civil Rights and Civil Liberties (CRCL)

DHS CRCL is available to help law enforcement with issues relating to the DHS mission and the protection of civil rights and civil liberties. CRCL works with other DHS offices and components to develop policies, programs, and training material. It also investigates complaints alleging violation of rights, programs, or policies by DHS employees, leading to recommendations to fix identified problems and help DHS safeguard the nation while preserving individual liberty, fairness, and equality under the law.

CRCL is also responsible for assuring that the Department's federally-assisted programs comply with various civil right laws, including but not limited to Title VI of the Civil Rights Act of 1964, as amended; Title IX of the Education Amendments of 1972, as amended; and the Rehabilitation Act of 1973, as amended.

Civil Rights Requirements in Federally-Assisted Programs. CRCL provides resources, guidance, and technical assistance to recipients of DHS financial assistance on complying with Title VI of the Civil Rights Act of 1964 (Title VI) Section 504 of the Rehabilitation Act of 1973, and related statutes.
Information for recipients on meeting their nondiscrimination requirements under Title VI is available on CRCL's website, www.dhs.gov/title-vi-overview-recipients-dhs-financial-assistance.

CRCL also published guidance to help those who carry out Department-supported activities to understand and implement their obligations under Title VI to provide meaningful access for people with limited English proficiency (www.dhs.gov/guidance-published-help-department-supported-organizations-provide-meaningful-access-people-limited). For more information, please contact crcl@hq.dhs.gov.

Common Muslim American Head Coverings and Common Sikh American Head Coverings Posters provide guidance to Department personnel on the appropriate ways in which to screen and, if necessary, search Muslim or Sikh individuals wearing various types of religious head coverings. Although these posters are primarily designed for DHS personnel, they are available to state and local law enforcement.
For more information, visit www.dhs.gov/civil-rights-and-civil-liberties-institute.

Educational posters in customizable digital and hard copy form can be ordered from the DHS CRCL by emailing crcltraining@hq.dhs.gov.

Community Roundtables. CRCL leads, or plays a significant role, in regular roundtable meetings across the country in over 14 U.S. cities. These roundtables bring exceptionally diverse demographic communities together with federal, state, local, tribal, and territorial government representatives. Issues discussed range from immigration and border issues to civil rights issues in aviation security. CRCL also conducts roundtables with young leaders of diverse communities. For more information, contact communityengagement@hq.dhs.gov.

Countering Violent Extremism (CVE) Training Guidance and Best Practices. This written guidance provides best practices for federal, state, and local government and law enforcement officials organizing CVE, cultural awareness, and counterterrorism training.
For more information, visit www.dhs.gov/civil-rights-and-civil-liberties-institute.

CRCL Impact Assessments review Department programs, policies, and activities to determine whether these initiatives have an impact on the civil rights and civil liberties of those affected by the initiative. For more information about CRCL Impact Assessments, visit www.dhs.gov/crcl.

DHS Complaint Avenues Guide. DHS has many avenues for the public to make complaints involving DHS employees or programs, alleged violations of civil rights and civil liberties, immigration filing, travel redress, and other types of grievances. CRCL developed a guide which brings together information about these avenues. For more information, visit: http://www.dhs.gov/sites/default/files/publications/dhs-complaint-avenues-guide_10-03-12_0.pdf

CRCL Newsletter is distributed monthly to inform stakeholders and the public about office activities, including how to make complaints; ongoing and upcoming projects; and opportunities to offer comments and feedback. Newsletters are distributed via an email list to thousands of non-governmental organizations, community members, and government partners, and made available to community groups for redistribution. For more information, visit http://www.dhs.gov/publication/crcl-newsletter.

Guidance Regarding Use of Race for Law Enforcement Officers. Developed by CRCL in partnership with the Department of Justice (DOJ), this training reviews the DOJ guidance regarding racial profiling.
Duration: 20 minutes. CD-ROMs can be ordered from CRCL by emailing crcltraining@hq.dhs.gov.

How to File and Submit a Complaint. Under 6 U.S.C. § 345 and 42 U.S.C. § 2000ee-1, CRCL reviews and assesses information concerning abuses of civil rights, civil liberties, and profiling on the basis of race, ethnicity, or religion, by employees and officials of DHS. Complaints are accepted in languages other than English. For more information, visit www.dhs.gov/crcl.

Introduction to Arab American and Muslim American Cultures is an hour-long training DVD, released in the fall of 2006, that provides insights from four national and international experts, including an Assistant U.S. Attorney who is a practicing Muslim; a member of the National Security Council who is a practicing Muslim; a scholar of Islamic studies; and a civil rights attorney who advocates on issues of concern to Arab American and Muslim American communities. The training assists law enforcement officers and other personnel who interact with Arab and Muslim Americans, as well as individuals from Arab or Muslim communities in the course of their duties. For more information, visit http://www.dhs.gov/civil-rights-and-civil-liberties-institute or contact crcltraining@hq.dhs.gov.

"I Speak" Language Identification Pocket Guides and Posters. CRCL has created a set of three tools ("I Speak" poster, pocket guide, and job aid) for use by state and local law enforcement officers and sheriffs who work directly with the public and who may need to identify the language of the person with whom they are interacting. These tools support the Limited English Proficiency plans that many sheriff's offices have put in place to meet the requirements of Title VI of the Civil Rights Act. The "I Speak" format includes 75 of the most frequently encountered languages, as well as 13 of the indigenous languages of Mexico and Central America. For more information, digital copies, samples, or customization of a low literacy version, email crcltraining@hq.dhs.gov.

Privacy, Civil Rights & Civil Liberties Fusion Center Training Program. The Implementing Recommendations of the 9/11 Commission Act requires that DHS support fusion centers by providing training on privacy, civil rights, and civil liberties. As a result, CRCL and the DHS Privacy Office have partnered with the DHS Office of Intelligence & Analysis and the

DOJ Bureau of Justice Assistance to deliver this training program. The program has included: A website resource center www.it.ojp.gov/PrivacyLiberty; a training of Privacy/Civil Liberties Officers program; a technical assistance program; and an on-site training program. Topics covered include: civil rights and civil liberties basics and red flags (how to spot potential issues and incorporate safeguards into your procedures); privacy fundamentals (how to integrate your privacy policy and recognize and respond to a privacy incident); cultural tactics for intelligence and law enforcement professionals (covers frequently encountered misconceptions and stereotypes and addresses policies against racial or ethnic profiling); and First Amendment issues in the information sharing environment (covers considerations when fusion centers may encounter constitutionally protected activities, such as freedom of speech, demonstrations, petitions for redress, etc.). Fusion centers and their liaison officer networks have the option of choosing additional topics to create a customized agenda. Technical assistance is also available. *Duration*: Full-day (eight hours) but can be customized to shorter sessions. For more information, email FusionCenterTraining@hq.dhs.gov.

The First Three to Five Seconds: Arab and Muslim Cultural Awareness for Law Enforcement. This course is intended to help law enforcement personnel to better understand the culture of Arab and Muslim Americans, including topics such as why an individual's name may differ among documents and general background on Islam in the United States. This video was developed by the DOJ Community Relations Service and reproduced by DHS. *Duration*: 10 minutes.

For more information, visit www.dhs.gov/civil-rights-and-civil-liberties-institute. This site also offers a transcript and limited resources and glossary. You may order DVDs from CRCL by emailing crcltraining@hq.dhs.gov.

Web Portal for Privacy and Civil Rights & Civil Liberties Officers. This portal provides training materials and video resources for state and local personnel and trainers on privacy, civil rights, and civil liberties issues encountered by fusion centers and justice entities. The recently updated web portal includes over 30 pages of new content specifically geared toward privacy and civil rights and civil liberties officers. The portal was developed as a result of a partnership between CRCL, Privacy Officers, and the DHS Office of Intelligence and Analysis.

Available at: www.it.ojp.gov/PrivacyLiberty.

United States Coast Guard (USCG)

USCG has a wide array of surface, air, and specialized assets and capabilities available for multiple levels of response, patrol, and mission specific tasks.

Surface platforms consist of boats and larger cutters. Vessels under 65 feet in length are classified as boats and usually operate near shore on inland waterways and from cutters. Craft include: Motor Lifeboats; Medium and Small Response Boats; special purpose response boats; port security boats; Aids to Navigation boats; and a variety of smaller, non-standard boats including rigid hull inflatable boats. Sizes range from 64-foot in length down to 12-foot. Cutters are basically any commissioned USCG vessel 65 feet in length or greater, having adequate accommodations for crew to live onboard. Cutters usually have one or more rigid hull inflatable boats onboard. Polar Class icebreakers also carry an Arctic Survey Boat and Landing Craft. The USCG cutter fleet ranges from a 420-foot Icebreaker to a 65-foot harbor tug, however, most commonly recognized and widely utilized are National Security Cutters, High and Medium Endurance Cutters (420-foot, 378-foot, 270-foot, and 210-foot) and our smaller 87-foot Marine Protector Class,110-foot Island Class, and 154-foot Sentinel Class patrol vessels.

There are a total of 190 aircraft in Coast Guard inventory, a figure that will fluctuate due to operational and maintenance schedules. Major Missions consist of Search/Rescue, Law Enforcement, Environmental Response, Ice Operations, and Air Interdiction. Fixed-wing aircraft (C-130 Hercules and C-144 Ocean Sentry turboprops) operate from large and small Air Stations. Rotary wing aircraft (H-65 Dolphin and HH-60 Jayhawk helicopters) operate from flight-deck equipped Cutters, Air Stations, and Air Facilities.

USCG Deployable Specialized Forces (DSF) provides additional teams and resources such as Maritime Safety and Security Teams (11), Port Security Units (8), Tactical Law Enforcement Teams (2), Maritime Security Response Team (1), National Strike Force and Regional Dive Lockers (2). DSF teams are capable of worldwide deployment via air, ground or sea transportation in response to changing threat conditions and evolving Maritime Homeland Security mission requirements. Core capabilities include: Enhanced Law Enforcement Boardings; Waterside Security/Force Protection; Landside Security/Force Protection; Port Security; Subsurface Operations; Chemical, Biological, Radiological, Nuclear and Enhanced Conventional Weapons (CBRNE) Detection and Identification; Disaster Response; Environmental Response; Deployable Incident Management; Advanced Planning; and multiple supporting capabilities.

America's Waterways Watch is a combined effort of the USCG and its Reserve and Auxiliary components to enlist the active participation of those who live, work, or play around America's waterfront areas. For more information, contact aww@uscg.mil or visit http://americaswaterwaywatch.uscg.mil. To report suspicious activity call 877-24WATCH (877-249-2824).

USCG Maritime Information eXchange ("CGMIX") makes USCG maritime information available to the public on the internet in the form of searchable databases. Much of the information on the CGMIX website comes from the USCG's Marine Information for Safety and Law Enforcement (MISLE) information system. For more information, visit http://cgmix.uscg.mil/.

USCG Navigation Center supports safe and efficient maritime transportation by delivering accurate and timely maritime information services and Global Position System (GPS) augmentation signals that permit high-precision positioning and navigation. For more information, visit http://www.navcen.uscg.gov/ or call 703-313-5900.

USCG Sector Command Centers. Given USCG mission diversity, asset readiness status and ongoing operations, the main avenue for proper and expeditious USCG asset mobilization requests are through USCG Sector Command Centers. There are 37 USCG Sectors.

Commands throughout the U.S. and U.S. territories:

Sector Command Centers

Sector Name	Locations	24/7 Contact
Anchorage	Anchorage, AK	907-428-4100
Baltimore	Baltimore, MD	410-576-2693
Boston	Boston, MA	617-223-5757
Buffalo	Buffalo, NY	716-843-9527
Charleston	Charleston, SC	843-740-7050
Columbia River	Warrenton, OR	503-861-6211
Corpus Christi	Corpus Christi, TX	361-939-6393
Delaware Bay	Philadelphia, PA	215-271-4940
Detroit	Detroit, MI	313-568-9560
Guam	Santa Rita, Guam	671-355-4824
Hampton Roads	Portsmouth, VA	757-668-5555
Honolulu	Honolulu, HI	808-842-2600
Houston-Galveston	Houston, TX	281-464-4854
Humboldt Bay	McKinleyville, CA	707-839-6123
Jacksonville	Atlantic Beach, FL	904-564-7511
Juneau	Juneau, AK	907-463-2980
Key West	Key West, FL	305-292-8727
Lake Michigan	Milwaukee, WI	414-747-7182
LA-Long Beach	San Pedro, CA	310-521-3600
Lower Mississippi	Memphis, TN	901-521-4822
Long Island	New Haven, CT	800-774-8724
Miami	Miami Beach, FL	305-535-4472
Mobile	Mobile, AL	251-411-6211
New Orleans	New Orleans, LA	800-874-2153
New York	Staten Island, NY	718-354-4120
North Bend	North Bend, OR	541-756-9220
North Carolina	Wilmington, NC	910-343-3880
Northern New England	South Portland, ME	207-767-0303
Ohio Valley	Louisville, KY	502-779-5400
Puget Sound	Seattle, WA	206-217-6001
San Diego	San Diego, CA	619-278-7000
San Francisco	San Francisco, CA	415-399-3300
San Juan	San Juan, PR	787-289-2041
Sault Ste Marie	Sault Ste Marie, MI	906-632-0967
Southeastern New England	Woods Hole, MA	508-457-3211
St Petersburg	St Petersburg, FL	727-824-7506
Upper Mississippi	St Louis, MO	314-269-2500

Office of Community Partnerships (OCP)

DHS has relaunched its Countering Violent Extremism (CVE) public webpage in 2014 and it will undergo further revision this year. On the webpage, individuals can find information about the Department's approach and resources such as a CVE tool-kit, information on "Building Communities of Trust", and information on how to apply for access to the DHS-FBI CVE Training Resources and Active Shooter Webportal. The webpage is further being updated with resources and relevant links. You can access the Department's CVE landing page at: http://www.dhs.gov/topic/countering-violent-extremism#.

Enhanced Engagement and Training Resources.
The Community Awareness Briefings (CAB)
To enhance engagement efforts and provide awareness training in regards to CVE, DHS, in partnership with the National Counterterrorism Center (NCTC), developed and is delivering the CAB. This briefing has been conducted in cities across the country to communities and state, local, and federal law enforcement.

The CAB is designed to share unclassified information regarding the threat of violent extremism. The CAB has been conducted in 14 U.S. cities over the past few years. It is designed to help communities and law enforcement develop the necessary understanding of al-Qa'ida, al-Shabaab, Islamic State of Iraq and the Levant (ISIL), and related affiliates' recruitment tactics and explore ways to collectively and holistically address these threats before they become a challenge at the local level. Due to the increased number of Western-based fighters traveling to foreign war conflicts, such as Syria and Somalia, the CAB now includes information relating to the foreign fighter recruitment narrative by al Shabaab and ISIL, and the myths versus realities of the situation in Syria and Somalia.

To learn more about the CAB please email: OSLLE@hq.dhs.gov.

U.S. Customs and Border Protection (CBP)

CBP is one of the DHS' largest and most complex components, with a priority mission of keeping terrorists and their weapons out of the United States. It also has a responsibility for securing the border and facilitating lawful international trade and travel while enforcing hundreds of U.S. laws and regulations, including immigration and customs laws. For more information, visit www.cbp.gov or contact 202-344-1700.

Carrier Liaison Program provides standardized training and assistance to international air carriers related to admissibility and fraudulent document detection in order to encourage carrier compliance with U.S. immigration laws. For more information about the Carrier Liaison Program, visit www.cbp.gov/travel/travel-industry-personnel/carrier-liaison-prog or contact CLP@dhs.gov or 202-621-7817.

CBP Border Community Liaison Program. Border Community Liaisons focus on outreach to community stakeholders and provide fact-based information regarding the CBP mission, functions, authorities, and responsibilities. Border Community Liaisons nationwide can be assessed through the CBP State, Local, Tribal Liaison Office at 202-325-0775 or by emailing CBP-STATE-LOCAL-TRIBAL-LIAISON@cbp.dhs.gov.

CBP Information Center provides general information about CBP requirements and procedures, as well as handling the intake for complaints related to CBP interactions. The CBP INFO Center also maintains an on-line database of Q&A's covering all aspects of customs and immigration operations. The CBP INFO Center can be reached at 877-CBP-5511 or 202-325-8000 or by visiting https://help.cbp.gov/app/home.

CBP Laboratories and Scientific Services coordinates technical and scientific support to all CBP and DHS-wide trade and border protection activities including laboratory analysis for trade enforcement and product safety, forensic services for criminal investigations, and 24/7 telephonic access to scientific resources for technical case adjudication for radiation/nuclear materials and other potential weapons of mass effect. For more information, visit www.cbp.gov\about\labs-scientific-svcs.

Intellectual Property Rights (IPR) Help Desk. CBP's IPR Help Desk provides information on IPR border enforcement procedures and receives allegations of IPR infringement. Questions regarding IPR enforcement at U.S. borders and information on IPR infringing goods that may be entering the U.S. can be directed to the IPR Help Desk at 562-980-3119 ext. 252, or via email at jpr.helpdesk@dhs.gov.

Missing or Late International Travelers. Information regarding reported missing or late international travelers can be obtained from the nearest port of entry. For a list of ports, visit http://cbp.gov/xp/cgov/toolbox/contacts/ports/.

No Te Engañes (Don't be Fooled) is the CBP outreach campaign to raise awareness of human trafficking among potential migrants. For more information, visit www.cbp.gov/xp/cgov/border_security/human_trafficking/no_te_enganes/ or contact Laurel Smith at laurel.smith@dhs.gov or 202-344-1582.

Port of Entry Information. CBP enforces the import and export laws and regulations of the U.S. Federal Government, processes international passengers and cargo, and performs agriculture inspections at ports of entry. Port personnel are the face at the border for most cargo and persons entering the United States. For a list of ports, visit http://cbp.gov/xp/cgov/toolbox/contacts/ports/.

Preventing International Non-Custodial Parental Child Abduction. DHS CBP partners with the Department of State's (DOS) Office of Children's Issues to prevent the international abduction of children involved in custody disputes or otherwise against the published order of the court. If you are concerned about the international travel of a child, please contact the DOS Office of Children's Issues at PreventAbduction@state.gov or the 24 hour hotline 888-407-4747.

State, Local and Tribal Liaison. A component of the CBP Commissioner's Office, the State, Local, and Tribal Liaison strives to build and maintain effective relationships with state, local, and tribal governments through regular, transparent, and proactive communication. Governmental questions regarding issues and policy pertaining to border security, trade, and facilitation can be referred to the SLT at CBP-STATE-LOCAL-TRIBAL-LIAISON@cbp.dhs.gov or 202-325-0775.

Suspicious Aircraft or Boats. The CBP Air and Marine Operations Center (AMOC) is responsible for securing the airspace at and beyond our Nation's borders through detection, monitoring, sorting and interdiction of general aviation and maritime threats. Suspicious air or maritime activity to include low flying aircraft and drug or human smuggling activity should be directed to AMOC at 1-866-AIRBUST.

Tip Line. Suspicious activity regarding international travel and trade can be reported to CBP at 1-800-BE-ALERT.

Visa Waiver Program (VWP) enables citizens and nationals from 38 countries to travel to and enter the U.S. for business or visitor purposes for up to 90 days without obtaining a visa. For more information about the Visa Waiver Program, visit http://www.cbp.gov/travel/international-visitors/visa-waiver-program.

Domestic Nuclear Detection Office (DNDO)

DNDO is a jointly staffed office within DHS. DNDO is the primary entity in the U.S. government for implementing domestic radiological and nuclear (R/N) detection efforts for a managed and coordinated response to R/N threats, as well as integration of federal nuclear forensics programs. DNDO is charged with coordinating the development of the global nuclear detection and reporting architecture, with partners from federal, state, local, tribal, territorial, and international governments and the private sector. For more information, visit www.dhs.gov/about-domestic-nuclear-detection-office or contact DNDO.INFO@hq.dhs.gov.

Equipment Test Results. Federal, state, local, tribal, and territorial agencies intending to purchase R/N detection equipment are strongly encouraged to consider instruments that have been independently tested by accredited laboratories and have demonstrated conformity with the applicable American National Standards Institute/ Institute of Electrical and Electronics Engineers (ANSI/IEEE) N42 standards. Manufacturers offering new equipment for consideration should be asked to provide evidence of independent testing for compliance with these standards. DNDO has resources that are available to assist federal, state, local, tribal, and territorial entities in selecting the right R/N detection equipment to meet their operational needs.

DNDO has conducted several equipment test campaigns to evaluate the effectiveness of detection systems in multiple performance areas to better support R/N detection procurement decisions and concept of operations development by federal, state, local, tribal, and territorial stakeholders.

These test campaigns have included detection system categories such as: radiation isotope identification devices (RIIDs), personal radiation detectors (PRDs), backpacks, and mobile systems (vehicle-mounted, boat-mounted, and aerial-mounted).

When test reports are completed and are available for release, federal, state, local, tribal, and territorial stakeholders are notified via DNDO Operations Support Directorate's weekly newsletter, *The Source*. To be added to the distribution list for *The Source*, simply email a request to DNDO.JAC2@hq.dhs.gov.

The **Data Mining, Analysis, and Modeling Cell** (DMAMC) is a team of subject matter experts from the radiation detection community responsible for leveraging existing data and analysis methods to answer scientific and technical questions posed by DNDO stakeholders related to the radiological detection mission. For more information contact the DMAMC at DMAMC@hq.dhs.gov

The GRaDER® Program. GRaDER® provides objective and reliable performance testing information to federal, state, and local stakeholders for R/N detection equipment tested against consensus and technical capability standards to assist in making informed R/N detection equipment procurements. For more information, visit www.dhs.gov/GRaDER or email GRaDER.questions@hq.dhs.gov.

Joint Analysis Center (JAC). The JAC, located within DNDO, provides awareness of the Global Nuclear Detection Architecture (GNDA) and provides technical support to federal, state, local, tribal, and territorial authorities. Utilizing the Joint Analysis Center Collaborative Information System (JACCIS), the JAC facilitates R/N alarm adjudication from detection events and consolidates and shares information and databases.

GNDA Awareness is achieved by establishing and maintaining links to detectors and access to Nuclear Regulatory Commission and Agreement State Material Licensing Data. GNDA Awareness also depends upon non-time critical requirements such as access to historical data on all detection events (illicit and legitimate) and access to information about commerce and related R/N infrastructure that affects detection assets and response protocols.

JACCIS provides federal, state, local, tribal, and territorial stakeholders adjudication connectivity, a detector database, and status information regarding the events and activities relating to R/N detection and nuclear forensics at the "Unclassified//For Official Use Only" level. In this capacity, JACCIS maintains awareness of the GNDA, which involves facilitating alarm adjudication and monitoring global efforts in R/N detection. JACCIS is completely web enabled so connectivity is possible anywhere in the country in real-time and utilizes an agile development process to release updates every quarter. The JAC provides information integration and analysis coupled with awareness of the GNDA. This enables the right information to be available at the point of detection and ensures that detection events result in either a proper response to a threat or a quick dismissal of a non-threat. To contact the JAC, call 866-789-8304 or e-mail DNDO.JAC2@hq.dhs.gov. For more information, visit www.dhs.gov/about-domestic-nuclear-detection-office.

Mobile Detection Deployment Units (MDDU). Collaboration between federal, state, local, tribal, and territorial law enforcement and public safety agencies is crucial to a layered approach to radiological and nuclear security. DNDO developed the MDDU as a surge asset to assist federal, state, local, tribal, and territorial agencies detect and report radiological and nuclear threats. The MDDU was designed to supplement radiological and nuclear detection capabilities in support of national and special security events, or in response to an intelligence-driven event.

MDDUs are mobile trailer packages containing radiation detection equipment for up to 40 public safety professionals. MDDU packages are prepositioned across the United States and are maintained and deployed for DNDO by U.S. Department of Energy (DOE) Radiological Assistance Program (RAP) personnel. The equipment includes personal radiation detection devices, portable backpack radiation detection units, high and low-resolution radiation identification hand-held instruments, mobile radiation detection systems, and interoperable communications and tracking equipment. Each MDDU is accompanied by DOE RAP technical support staff to train federal, state, local, tribal, and territorial personnel on the use of the specific MDDU equipment, and to help integrate these capabilities into existing operations.

Federal, state, local, tribal, and territorial agencies may request an MDDU by contacting DNDO at DNDO_MDDU_Request@hq.dhs.gov

Open Access to American National Standards Institute (ANSI) N42 Series Standards. DNDO sponsors the Institute of Electrical and Electronics Engineers (IEEE) to provide copies of the ANSI N42 Radiation Detection Standards free of charge to anyone who wants a copy. The website to obtain the latest published version of one of the sponsored standards is http://standards.ieee.org/about/get/.

Radiological and Nuclear Detection Exercises. DNDO's Exercises Program provides support in developing, designing, and conducting discussion or operational-based R/N detection exercises that are compliant with the Homeland Security Exercise and Evaluation Program methodology. Exercises provide valuable hands-on experience for federal, state, and local personnel performing R/N detection missions and assist decision makers in integrating the R/N detection mission into their daily operations. Additional information about R/N detection exercises is available by contacting DNDO at

DNDO.SLA@hq.dhs.gov.

Radiological /Nuclear Detection and Adjudication Capability Development Framework (CDF). The Capability Development Framework (CDF) provides guidance to federal, state, local, tribal, and territorial stakeholders to assist jurisdictions in identifying and developing recommended levels of R/N detection capability based on risk factors and the likelihood of encountering illicit R/N material. The CDF informs stakeholders of potential gaps in their ability to detect, report, and respond to R/N material outside of regulatory control. It is intended to provide strategic guidance based on best practices, but not to establish specific requirements. The CDF is a DNDO product that supports the Screening, Search, and Detection Core Capability and can be leveraged to support investment justifications. A CDF Calculator is also available to assist jurisdictions with identifying recommended levels of R/N detection capability quickly and easily. The CDF and supporting resources are available on the Homeland Security Information Network (HSIN) PRND Community of Interest (COI) web portal or by contacting DNDO.SLA@hq.dhs.gov.

Radiological/Nuclear Detection National Incident Management System (NIMS) Resource Types. DNDO coordinated the development of R/N detection resource types in partnership with federal, state, local, tribal, and territorial subject matter experts to support planning and organization, and increases efficiency and effectiveness for sharing R/N detection resources through the Emergency Management Assistance Compact and other mutual aid mechanisms. The NIMS-typed teams, equipment, and job titles provide a common categorization of R/N detection resources. FEMA is currently conducting a review to include these as national level tier one resources. The latest resource type definitions can be obtained by contacting DNDO.SLA@hq.dhs.gov.

Radiological and Nuclear Detection Community of Interest (COI). DNDO's R/N Detection COI is a site located on the Homeland Security Information Network (HSIN) that provides a repository of useful information on DNDO, PRND, the Global Nuclear Detection Architecture (GNDA), and other nuclear detection related activities that can be accessed by external users. It is also a forum where nuclear detection community stakeholders can securely collaborate and share best practices and lessons learned. State, local, tribal, and territorial law enforcement, fire, emergency management and radiation health personnel, federal agencies, federally-funded research and development centers, and academia directly supporting nuclear detection capability development at all levels of government are encouraged to join the site with other GNDA community stakeholders. To join the R/N Detection COI, submit a request by email to DNDO with a message subject line of: "DNDO RND COI HSIN Access Request" to the address: PRND_COI@hq.dhs.gov.

Radiological and Nuclear Detection Assistance Program. DNDO works with federal, state, local, tribal, and territorial government policy makers, program managers, and operational administrators to design, implement, and sustain a R/N detection program. DNDO's R/N Detection Assistance Program includes the development of concepts of operation, standard operating procedures, multiyear Training and Exercise Plans, Sustainment Plans, table top exercises (coordinated through the Exercises Program), and the sharing of lessons learned and best practices.

The program goal is to prevent the use of an R/N terrorist weapon against the interior or maritime portion of the United States. The Assistance Program seeks to establish sustainable R/N Detection capabilities among federal, state, local, tribal, and territorial agencies and emergency responders to detect and report unauthorized R/N materials out of regulatory control within their jurisdictions/regions. To request assistance or for more information on DNDO's Assistance Program, contact DNDO.SLA@hq.dhs.gov

Radiological and Nuclear Detection Training. DNDO's Training Program provides quality products to support, develop, enhance and expand R/N detection capabilities in support of the GNDA. Together with other federal partners, the DNDO Training Program provides instructional courses in basic, intermediate, advanced, and train-the-trainer R/N detection tactics, techniques, and procedures. The DNDO Training Program conducts technical review, evaluation, and continual developmental improvement of the R/N detection training curriculum. These reviews increase the operational detection capabilities of federal, state, local, tribal, and territorial agencies to detect and interdict R/N materials and/or devices. The program seeks to develop and implement protocols and training standards for effective use of R/N detection equipment and the associated alarm reporting and resolution processes. DNDO and its partners have completed R/N detection training for over 35,000 law enforcement, first responder personnel, and public officials through Fiscal Year 2015.

R/N detection training courses are available through FEMA's National Preparedness Directorate. Courses are taught by the National Domestic Preparedness Consortium member: Counter-Terrorism Operations Support (CTOS) – Center for Radiological/Nuclear Training. For more information, visit www.ctosnnsa.org/. Courses are also available through the FEMA Federal Sponsored Course catalog. FEMA FSCC Web page: www.firstrespondertraining.gov/webforms/pdfs/fed_catalog.pdf . For additional information regarding R/N detection training, visit https://gnda.energy.gov or email DNDO.SLA@hq.dhs.gov.

Securing the Cities (STC) Program. The STC Program assists state, local, and tribal stakeholders design and implement or enhance existing architectures for coordinated and integrated detection and interdiction of nuclear materials out of regulatory control that may be used as a weapon within high-threat/high-density Urban Area Security Initiative (UASI) areas. Urban Areas selected through a competitive application process. The program assists these jurisdictions by using cooperative agreements to enhance regional capabilities to detect, identify, and interdict nuclear materials that are out of regulatory control, guide the coordination of federal, state, local, and tribal entities in their roles defined by the GNDA and encourage participants to sustain their nuclear detection program over time. There are three phases to the program. In Phase I, STC assists state and locals in developing an initial operating capability to detect and report the presence of nuclear materials that are out of regulatory control. The initial regional capabilities are mutually supportive through cooperative agreements, region specific operations, interoperable equipment, collective training, and progressive exercise planning. In Phase II, STC provides additional resources to enhance detection, analysis, communication, and coordination to better integrate state and local capabilities with Federal government activities and the GNDA beyond Phase I. Finally, in Phase III, STC provides indirect support to sustain the program. DNDO works with regional partners to maintain connectivity with the established local architecture through alarm adjudication and subject matter expertise and provides advice on long-term training, exercise, and other program support. State and local participants will maintain and continue to improve their developed capabilities to support the GNDA using local funds or other Federal Government grant funds. For more information, email DNDOSTC@hq.dhs.gov.

Federal Emergency Management Agency (FEMA)

FEMA's mission is to support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

All-Hazards Emergency Planning Guides. In accordance with *Now is the Time: The President's Plan to Protect Our Children and Our Communities by Reducing Gun Violence*, FEMA along with DHS, and the Departments of Health and Human Services, Justice, and Education, collaboratively designed and published revised all-hazards emergency management planning guides that include sections that speak to the importance of preparing for, preventing, protecting against, mitigating, responding to, and recovering from an active shooter or mass casualty incident. This joint federal effort has resulted in the development of four guides designed for Houses of Worship, Institutions of Higher Education, Schools for Kindergarten through Twelfth Grade, U.S. Airports, and Medical Care Facilities. For more information and for electronic copies of the guides visit, www.fema.gov/plan.

The **Authorized Equipment List (AEL)**, published and maintained by the FEMA Grant Programs Directorate (GPD), is a tool used by grantees to determine allowability of equipment types for FEMA's Preparedness Grant Programs. The AEL is used to facilitate more effective and efficient procurement of items under specific FEMA Preparedness Grants by informing grantees of relevant standards, operating considerations and programmatic considerations associated with each equipment item. The AEL consists of 21 equipment categories, ranging from Personal Protective Equipment (PPE) to Medical Supplies to Terrorism Incident Prevention Equipment. The AEL exists with considerable overlap with the Standard Equipment List (SEL), a comprehensive list of first responder equipment maintained by the IAB, an inter-governmental group with representation from multiple federal agencies and the first responder community, and strong connections to subject matter experts in all equipment areas. GPD works in close collaboration with the IAB on the items and relevant information that is maintained on the AEL. The AEL has an interactive version which allows grantees to search for items by keyword, equipment category, or item number. Each item page includes the specific grant program(s) for which the item is allowable; a description of the item; and SEL data including operating considerations, item standards, and training information. For more information visit: http://beta.fema.gov/authorized-equipment-list.

Comprehensive Preparedness Guide 502: Considerations for Fusion Center and Emergency Operations Center Coordination provides state and major urban area fusion center and emergency operations center (EOC) officials with guidance for the coordination between fusion centers and EOCs. It outlines the roles of fusion centers and EOCs and provides steps by which these entities can work together to share information and intelligence on an ongoing basis. CPG 502 supports the implementation of the *Baseline Capabilities for State and Major Urban Area Fusion Centers*, and likewise, assists EOCs to fulfill their missions in both steady state and active state emergency operations. CPG 502 provides guidance on the broad capability requirements of an EOC. An electronic version of the guide is available at http://www.fema.gov/media-library/assets/documents/25970.

First Responder Training.

- Center for Domestic Preparedness (CDP), is DHS's only Federally-chartered Weapons of Mass Destruction (WMD) training center committed to having an emergency response community prepared for and capable of responding to all-hazards events. The interdisciplinary resident and nonresident training courses at CDP promote a greater understanding among the diverse responder disciplines: Emergency Management, Emergency Medical Services, Fire Service, Governmental Administrative, Hazardous Materials, Healthcare, Law Enforcement, Public Health, Public Safety Communications, and Public Works.

- Emergency Management Institute (EMI) serves as the national focal point for the development and delivery of emergency management training to enhance the capabilities of state, local, tribal, and territorial government officials; volunteer organizations; FEMA's disaster workforce; other federal agencies; and the public and private sectors to minimize the impact of disasters and emergencies on the American public.

- National Exercise Program (NEP) serves as the principal mechanism for examining the preparedness and readiness of the United States across the entire homeland security and management enterprise. The purpose of the NEP is to design, coordinate, conduct, and evaluate exercises that rigorously test the Nation's ability to perform missions and functions that prevent, protect against, respond to, recover from, and mitigate all hazards. As a component of the National Preparedness System, the NEP provides a consistent method to examine and validate federal and whole community partner core capabilities, which in turn indicate the Nation's progress in reaching the National Preparedness Goal (Goal).

  Each Program cycle consists of a two-year, progressive schedule of exercises that are selected based on their support to the Goal, and the Program's Principals' Objectives. The types of exercises selected into the program may include facilitated policy discussions, seminars and workshops, tabletop exercises, modeling and simulation, drills, functional exercises, and full-scale exercises. All of which may be sponsored by organizations from any level of government, non-governmental and private sector, and the whole community.

- National Training and Education Division (NTED) serves the nation's first responder community, offering more than 150 courses to help build critical skills that responders need to function effectively in mass consequence events. NTED primarily serves state, local, territorial, and tribal entities in 18 professional disciplines. Instruction is offered at the awareness, performance, and management and planning levels. Students attend NTED courses to learn how to apply the basic skills of their profession in the context of preparing, preventing, deterring, responding to and recovering from acts of terrorism and catastrophic events. Course subjects range from weapons of mass destruction terrorism, cybersecurity, and agro-terrorism to citizen preparedness and public works. NTED training includes multiple delivery methods: instructor-led (direct deliveries), train-the-trainers (indirect deliveries), customized (conferences and seminars) and web-based. Instructor-led courses are offered in residence (i.e., at a training facility) or through mobile programs, in which courses are brought to state and local jurisdictions that request the training.

Joint Counterterrorism Awareness Workshop Series (JCTAWS). The Joint Counterterrorism Awareness Workshop Series (JCTAWS) is a nationwide initiative designed to improve the ability of local jurisdictions to detect, prevent, and disrupt terrorist activities.

JCTAWS have been held more than 16 major cities across the U.S., bringing together Federal, state, and local participants from across the law enforcement, fire, emergency response, medical services, and private sector communities to include hospital and medical personnel. The workshops, emphasizing the state and local response, delve into the challenges presented by both the operational and medical responses, and aim to review existing preparedness, response and interdiction plans, policies, and procedures related to a complex terrorist attack; identify gaps in plans, operational capabilities, response resources, and authorities; examine healthcare system challenges unique to a complex attack; strategize about community and bystander assistance to the wounded and consider providing medical management nearer to the attack site; and identify federal, state, and local resources—including grants, training, exercises, and technical assistance—available to address potential gaps in capabilities.

Office of the Law Enforcement Advisor. The mission and role of FEMA's Senior Law Enforcement Advisor is to enhance communication and coordination between FEMA and the law enforcement community and provide the Administrator and Agency with a law enforcement perspective on plans and policies and to support the agency's integration of law enforcement, public security, and emergency management communities.

Preparedness (Non-Disaster) Grant funding in the form of formula and competitive grants to enhance the capacity of state, local, tribal, territorial, and private sector emergency responders to prevent, protect against, respond to, and recover from a weapon of mass destruction, terrorism incident involving chemical, biological, radiological, nuclear, explosive devices, and cyber-attacks as well as other disasters. For more information on how to find and apply for grants visit www.fema.gov/preparedness-non-disaster-grants or www.Grants.gov.

Protection and National Preparedness contributes to the development and implementation of preparedness doctrine that reaches federal state, local, tribal, and territorial emergency management communities, as well as non-government entities and the private sector. The guidance and doctrine includes the National Preparedness Goal and National Preparedness System, National Incident Management System, and National Planning Frameworks.

- Within its National Preparedness Directorate, the National Integration Center examines emerging technologies, develops state and local planning guidance, provides technical assistance, and supports resource typing and the credentialing of emergency response personnel.
- Within its National Continuity Programs, FEMA provides guidance and tools for continuity at all levels of government and communications systems. Continuity of Operations is an effort within departments and agencies to ensure that Primary Mission Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.
- The **Integrated Public Alert and Warning System (IPAWS)** is a national FEMA-managed system that public safety officials can use to send public information and warning messages to people in a specific geographic area. IPAWS connects authorities at the federal, state, local, tribal, and territorial level and enables sending of Wireless Emergency Alert (WEA) messages to cell phones, Emergency Alert System (EAS) broadcasts to radio and TV, non-weather emergency message broadcasts over NOAA All-Hazards Weather Radio, and internet applications and websites that support alert

and warning distribution. IPAWS provides emergency information to people without an understanding of the English language and facilitates delivery of emergency information to people with access and functional needs. IPAWS is also connected with the Canadian Multi-Agency Situational Awareness System to enable sharing of alert, warning, and incident information across borders to improve response coordination during binational disasters. Additional information and inquiries about IPAWS and requirements for becoming an IPAWS user can be directed to the IPAWS Program Office at IPAWS@fema.dhs.gov.

Federal Law Enforcement Training Centers (FLETC)

***Contact Information*:**
Federal Law Enforcement Training Centers
Address: 1131 Chapel Crossing Road, Bldg. 2200, Glynco, GA 31524

Web Site: https://www.fletc.gov/state-local-tribal
E-mail: stateandlocaltraining@dhs.gov

The FLETC offers advanced and specialized law enforcement training in a variety of topics through the State, Local, and Tribal Division (SLTD), to state, local, and tribal law enforcement officers throughout the U.S. and Indian country/jurisdictions. The programs SLTD delivers are developed with the advice, assistance, and support of federal, state, local, and tribal law enforcement agencies and are updated to ensure relevance to today's issues. They are conducted at selected venues throughout the country hosted by a local law enforcement agency or at one of FLETC's training delivery points which are located in Artesia, NM; Charleston, SC; Cheltenham, MD; and Glynco, GA. Tuition, lodging, and meals assistance may be available to state, local, and tribal officers, but attendance is on a "space-available" basis. To learn more about FLETC training courses available to state, local, and tribal law enforcement and for contact information visit https://www.fletc.gov/state-local-tribal or contact stateandlocaltraining@dhs.gov**.**

The **FLETC Online Campus** is a secure online Academic Learning Management System (ALMS) developed by the FLETC in support of the law enforcement learning environment. The Online Campus currently offers over 100 professionally developed interactive online courses that are available for U.S. sworn and vetted law enforcement officers and agents. The Online Campus registration and access to course materials is provided through the Regional Information Sharing System (RISS), law enforcement officers and agents are required to complete the RISS Automated Trusted Information Exchange Application™ (ATIX) applicaiton. For more information, visit www.fletc.gov/e-fletc-online-campus.

Office of Health Affairs (OHA)

OHA serves as DHS's principal authority for all medical and health issues. OHA provides medical, public health, and scientific expertise in support of the DHS mission to prepare for, respond to, and recover from all threats. OHA serves as the principal advisor to the Secretary and the Federal Emergency Management Agency (FEMA) Administrator on medical and public health issues. OHA leads the Department's workforce health protection and medical oversight activities. The office also leads and coordinates the Department's biological and chemical defense activities and provides medical and scientific expertise to support the Department's preparedness and response efforts.

OHA has four strategic goals that coincide with the strategic goals of the Department:

- Provide expert health and medical advice to DHS leadership;
- Build national resilience against health incidents;
- Enhance national and DHS medical first responder capabilities; and
- Protect the DHS workforce against health threats.

For more information on OHA resources for support to state and local law enforcement, please send an e-mail to HealthAffairs@dhs.gov, or NOC.OHA@hq.dhs.gov.

BioWatch is a nationwide biosurveillance monitoring system operating in more than 30 metropolitan areas across the country that is designed to detect the release of select aerosolized biological agents. OHA provides program oversight for the BioWatch program while state and local agencies operate the system in their jurisdictions. BioWatch is a collaborative effort of multidisciplinary partners at the federal, state, and local level, including public health, laboratory, environmental agencies, emergency management, and law enforcement. Jurisdictional preparedness and response planning efforts related to the BioWatch program are developed through these partnerships. Biowatch partnerships bring experts at every level of government together to enhance resilience.

The **First Responder Guidance for Improving Survivability in Improvised Explosive Device (IED) and/or Active Shooter Incidents** was developed at the request of the National Security Council's working group on IED situations and in response to first responders who have encountered mass casualties from IEDs and/or active shooter incidents. Led by OHA Medical First Responder Coordination Branch, the guide was developed in coordination with the Departments of Defense, Health and Human Services, Justice, and Transportation. The Guide is available electronically at http://www.dhs.gov/publication/iedactive-shooter-guidance-first-responders.

The **National Biosurveillance Integration Center (NBIC)** integrates biosurveillance activities across the human health, animal, plant, food, water, and environmental domains to provide a biological common operating picture and facilitate earlier detection of adverse events and trends. NBIC works in partnership with federal, state, local, territorial, tribal, and private sector partners to synthesize and analyze information collected from across the spectrum of these organizations to provide more rapid identification of and response to biological threats. NBIC shares this information with stakeholders via the DHS Common Operating Picture (COP), providing a comprehensive electronic picture with assessments of current biological events, trends, and their potential impacts on the Nation's homeland security. Additionally, access to state and local NBIC Biosurveillance Reports are available on the Homeland Security Information Network (HSIN) to public health, health care, agriculture, environment, and law enforcement personnel across the country at all levels of government. To request access to HSIN-NBIC-SL, contact nbicoha@hq.dhs.gov.

U.S. Immigration and Customs Enforcement (ICE)

ICE's primary mission is to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. The agency has an annual budget of approximately $6 billion dollars, primarily devoted to its two operational directorates – ICE Homeland Security Investigations (HSI) and ICEEnforcement and Removal Operations (ERO).

Toolkit for Prosecutors. To demonstrate its commitment to strengthening coordination with state and local prosecutor partners, ICE developed the Toolkit for Prosecutors. This Toolkit is aimed at helping prosecutors navigate situations where important witnesses, victims, or defendants may face removal because they are illegally present in the United States. For more information, visit www.ice.gov/doclib/about/offices/osltc/pdf/tool-kit-for-prosecutors.pdf.

Victim Assistance Program (VAP) provides information and assistance to victims of federal crimes, including human trafficking, child exploitation, human rights abuse, and white collar crime. VAP also provides information to victims on post-correctional release or removal of criminal aliens from ICE custody. VAP has developed informational brochures on human trafficking victim assistance, crime victims' rights, white collar crime, and the victim notification program. For further information, please contact VAP at victimassistance.ice@dhs.gov or 866-872-4973.

ICE ENFORCEMENT AND REMOVAL OPERATIONS (ERO)

The **287(g) Program** allows a state or local law enforcement entity to enter into a partnership with ICE, under a joint Memorandum of Agreement (MOA), in order to receive delegated authority for immigration enforcement within their jurisdictions. In many cases, criminal activity is most effectively combated through a multi-agency/multi-authority approach that brings together the skills and expertise of federal, state, and local resources. State and local law enforcement agencies play a critical role in protecting our national security because the vast majority of criminals are taken into custody under their jurisdiction. The 287(g) Fact Sheet provides information regarding the 287(g) program. For more information, visit https://www.ice.gov/factsheets/287g.

The **Criminal Alien Program (CAP)** provides ICE-wide direction and support in the biometric and biographic identification, arrest, and removal of priority aliens who are incarcerated within federal, state, and local prisons and jails, as well as at-large criminal aliens that have circumvented identification. The identification and processing of incarcerated criminal aliens, before release from jails and prisons, decreases or eliminates the time spent in ICE custody and reduces the overall cost to the Federal Government. Additionally, ICE ERO, in conjunction with the Offices of the United States Attorneys, actively pursues criminal prosecutions upon the discovery of offenses of the nation's criminal code and immigration laws. This further enhances public safety and provides a significant deterrent to recidivism. Additional information on CAP may be found at https://www.ice.gov/criminal-alien-program.

ICE Enforcement and Removal Operations 101 (ERO 101) is a PowerPoint presentation compiled to introduce ICE ERO and its program offices. Though the slides themselves are not accessible to the public, the presentation can be delivered by any field office upon request. ICE ERO 101 is a condensed overview of ICE ERO programs and initiatives and is updated quarterly. In addition, each field office has area of responsibility-specific slides to accompany the overall ICE ERO 101 in order to provide a more focused look at ICE ERO in the local area. To find the nearest field office, visit https://www.ice.gov/contact/ero

ICE ERO Most Wanted Program is managed by the National Fugitive Operations Program (NFOP) as a vital tool to support ICE ERO's efforts in the location and arrest of the most dangerous fugitives and at-large criminal aliens. The Most Wanted Program serves as a force multiplier by focusing additional resources on the most egregious offenders, develops community support by providing visibility and fostering awareness of ICE ERO's public safety mission, and builds cooperative relationships with law enforcement partners though the exchange of mutually beneficial information aimed at removing these threats from local communities. More information on the NFOP can be found at www.ice.gov/fugitive-operations and http://www.ice.gov/most-wanted.

ICE-INTERPOL Fugitive Alien Removal (FAR) Initiative. The FAR Initiative seeks to locate, arrest, and remove foreign fugitive aliens at-large in the United States. A "foreign fugitive" is a removable alien with an arrest warrant from a foreign country for an offense which is also considered a crime in the United States. ICE Liaisons at INTERPOL assist in confirming criminal wants and warrants from foreign countries, developing investigative leads, and sharing information with law enforcement partners across borders. The ICE Liaisons at the INTERPOL Alien/Fugitive Division can be contacted at 202-532-4297 or 202-616-2416. The INTERPOL Operations and Commaactind Center can be reached at 202-616-3900 or INTERPOL.ALIENFUGITIVEDIVISION@ice.dhs.gov.

Joint Effort Initiative. The Joint Effort Initiative combines the resources and expertise of ICE ERO with local law enforcement agencies to help make communities safer. The purpose of this initiative is to promote community safety through the arrest and removal of criminal aliens and members of transnational street gangs. Working in a support role to local law enforcement, ICE ERO responds to situations where there is believed to be a criminal and immigration nexus, and provides investigative and enforcement support with the goal of reducing crime. Individual ICE ERO officers or a Fugitive Operations Team can embed with a state or local law enforcement agency on a part-time basis or in a full-time capacity. More information on the Joint Effort Initiative can be found at www.ice.gov/fugitive-operations.

Law Enforcement Information Sharing Initiative (LEISI) facilitates the sharing of DHS sensitive but unclassified law enforcement information with other federal, tribal, state, local, and international law enforcement agencies. LEISI provides the electronic Law Enforcement Information Sharing Service (LEIS Service) that other law enforcement agencies can utilize to query records pertaining to ICE criminal subjects and ICE and CBP immigration violators. For more information, contact LEISI at DHS-LEISI@ice.dhs.gov.

Law Enforcement Support Center (LESC), administered by ICE ERO, is a critical point of contact for the national law enforcement community, providing a wide range of information services to officers and investigators at federal, state, and local levels. The LESC operates 24 hours a day; 365 days a year to provide timely, accurate and real-time assistance to law enforcement agencies that are in need of the immigration status and identities of a foreign national that has been encountered, arrested or is under investigation for criminal activity.

To support these law enforcement efforts, the most efficient method to request and receive immigration information is by submitting an Immigration Alien Query (IAQ) to the LESC. The IAQ is generated in two ways; either an automated biometric (fingerprints) submission or a biographic, initiated by utilizing the International Justice and Public Safety Network (Nlets), message key IAQ at VTICE0900. Direct contact can also be made via the Law Enforcement Hotline at 1-802-872-6020. For additional information, visit www.ice.gov/lesc.

The **Pacific Enforcement Response Center (PERC)** provides 24/7 mission critical support to ICE field offices by delivering near real-time detainer issuance, intelligence support, and proactive and risk-based targeting of removable criminal aliens. This is accomplished through interoperability and the information sharing capabilities of the PERC, the LESC, and the FBI's Next Generation Initiative (NGI) fingerprint database. The PERC's proactive targeting focuses on removable criminal aliens who pose a threat to national security and public safety. Real-time intelligence is disseminated to field offices in the form of actionable leads associated with criminal aliens in federal/state/local custody and at-large aliens. In addition, the PERC provides critical information to INTERPOL, Joint Terrorism Task Forces, and other Federal law enforcement partners in furtherance of shared public safety and national security missions. The PERC can be contacted directly 24/7 by calling the Law Enforcement Line at 949-360-4500.

The **Priority Enforcement Program (PEP)** focuses on individuals convicted of significant criminal offenses or who otherwise pose a threat to public safety, such as gang members. Under PEP, ICE will only seek transfer of individuals in state and local custody in specific, limited circumstances. ICE will only issue a detainer where an individual fits within DHS'snarrower enforcement priorities and ICE has probable cause that the individual is removable. In many cases, rather than issue a detainer, ICE will instead request notification (at least 48 hours, if possible) of when an individual is to be released. ICE will use this time to determine whether there is probable cause to conclude that the individual is removable and arrange for the safe and orderly transfer of the criminal alien from the state or local law enforcement agency. Additional information on PEP may be found at https://www.ice.gov/pep.

National Criminal Analysis and Targeting Center (NCATC). As part of ICE ERO's Targeting Operations Division, the NCATC analyzes data and develops lead and information referrals for law enforcement. The information is used to locate and arrest criminal and other priority aliens who pose a threat to our nation's communities. By leveraging technology and partnerships with domestic and international law enforcement, regulatory, and intelligence agencies, the NCATC provides a specialized law enforcement workforce that analyzes the nature and characteristics of the removable alien population. The NCATC, in coordination with other ICE ERO and ICE enforcement entities, serves as an operational component of ICE's cooperative and community safety-based concept.

National Fugitive Operations Program (NFOP) was established to locate and arrest removable aliens who are at-large within the United States. The 129 Fugitive Operations Teams (FOTs) across the nation prioritize their investigations on national security cases and transnational gang members, convicted criminals and sex offenders, visa violators, and aliens with removal orders who have failed to depart the United States. FOT members work together with law enforcement partners and on interagency task forces to offer immigration enforcement expertise and pursue a common public safety strategy. For more information, visit www.ice.gov/fugitive-operations.

Online Detainee Locator System (ODLS) is a public system available online at www.ice.gov that allows family members, legal representatives, and members of the public to locate immigration detainees who are in ICE detention. As part of detention reform, ICE deployed the ODLS so that family members and attorneys can locate detainees more easily online, 24 hours a day, seven days a week. The system is available in eight different languages, with more languages to come. The ODLS can be searched in two ways: 1) by Alien Registration number (or A-number, the nine-digit identification number assigned to a person who applies for immigration benefits or is subject to immigration enforcement proceedings); or 2) by last name, first name, and country of birth. For more information, visit https://locator.ice.gov/odls/homepage.do

Probation and Parole Enforcement entails the identification and arrest of foreign born nationals who have been convicted of crimes and released from incarceration (paroled), or have been placed on probation without incarceration and released into the community under supervision. This is an essential immigration enforcement function of ICE in carrying out its public safety mission. ERO Officers and Fugitive Operations Teams work closely with probation and parole agencies to serve as a force multiplier, provide an open exchange of information, and fulfill common community safety objectives.

ICE HOMELAND SECURITY INVESTIGATIONS (HSI)

Border Enforcement Security Task Force (BEST). In response to a significant increase in violence along the Southwest border, ICE HSI, in partnership with U.S. Customs and Border Protection (CBP), as well as other federal, state, local, tribal, territorial, and international law enforcement officials have expanded its ongoing Border Crimes Initiative by creating BEST, a multi-agency initiative. To date, a total of 37 BESTs have been initiated across 16 states and in Puerto Rico. These teams are comprised of over 1,000 members who represent over 100 law enforcement agencies that have jointly committed to investigate transnational criminal activity along the Southwest Border, Northern Border, and at our nation's major seaports. For more information, visit www.ice.gov/best/.

Cultural Property, Art and Antiquities Program (CPAA) oversees investigations involving the illicit trafficking of cultural property from countries around the world and facilitates the repatriation of these objects to their rightful owners. United States federal importation laws regarding smuggling and trafficking provide ICE HSI special agents the authority, jurisdiction, and responsibility to take the leading role in criminal investigations that involve the illicit importation and distribution of stolen or looted cultural property and prosecuting those responsible for these crimes. When contacting ICE HSI to report instances of illicit importation and distribution of cultural property, please provide as much detailed information and supporting documentation as possible, including the following: a detailed description of the artifact and location (pictures if possible); a full statement of the reasons for the belief that the artifact may be or has been imported into the United States due to the illicit importation from (1) country of origin (if known) or (2) distribution from an archeological site in the United States (if known). For more information, visit http://www.ice.gov/cultural-art-investigations. Reports may be sent to HSIculturalproperty@ice.dhs.gov.

Cyber Crimes Center (C3), a component of ICE HSI, was established in 1997 for the purpose of combating crimes committed on, or facilitated by, the Internet. C3 is ICE HSI's main focal point for coordinating the agency's cyber strategy as it relates to cybercrime and computer forensics. ICE HSI's main strategy for cybercrime is to combat transnational cybercrime threats and the criminal exploitation of the Internet by investigating, disrupting and dismantling transnational criminal organizations and other malicious actors engaged in high-impact or far-reaching cybercrime, as well as provide training, guidance, and assistance to ICE HSI offices located throughout the world.

C3 is comprised of the Cyber Crimes Unit (CCU), the Child Exploitation Investigation Unit (CEIU), and the Computer Forensics Unit (CFU). This state-of-the-art center offers cyber-crime support and training to federal, state, local and international law enforcement agencies. C3 also includes a fully equipped computer forensics laboratory, which specializes in digital evidence recovery. For more information, visit http://www.ice.gov/cyber-crimes/.

Document and Benefit Fraud Task Forces (DBFTF). ICE HSI leads 23 interagency task forces across the United States. Individual task forces are comprised of federal, state, and/or local law enforcement partners working together to combat immigration document and benefit fraud, as well as related criminal violations. DBFTF locations include Atlanta, Baltimore, Boston, Buffalo, Chicago, Dallas, Denver, Detroit, Harlingen, Houston, Honolulu, Los Angeles, Miami, New York, Newark, Orlando, Philadelphia, Sacremento, Salt Lake City, San Francisco, San Juan, St. Paul, and Washington D.C. Through collaboration and partnership with multiple federal, state, and local agencies, the DBFTFs maximize resources, eliminate duplication of efforts, and produce a strong law enforcement presence. They combine ICE HSI's unique criminal and administrative authorities with a variety of other law enforcement agencies' tools and authorities to achieve focused, high-impact criminal prosecutions and financial seizures. Partners include U.S. Citizenship and Immigration Services, Fraud Detection and National Security; U.S. Department of State, Diplomatic Security; U.S. Department of Labor, Office of the Inspector General; U.S. Social Security Administration, Office of the Inspector General; U.S. Postal Inspection Service; U.S. Secret Service and numerous state and local law enforcement agencies. Supporting these task forces is the ICE HSI Forensic Laboratory, and the ICE HSI Cyber Crimes Center (C3). For more information, visit www.ice.gov/document-benefit-fraud/.

Forced Labor Program. ICE HSI investigates allegations of forced labor in violation of the Tariff Act of 1930 (Title 19 USC §1307), relating to the illegal importation of goods mined, manufactured, or produced, wholly or in part, through the use of forced labor, prison labor, and/or indentured labor under penal sanctions. When contacting ICE to report instances of forced labor, please provide as much detailed information and supporting documentation as possible, including the following: a full statement of the reasons for the belief that the product was produced by forced labor and that it may be or has been imported into the United States; a detailed description of the product; and all pertinent facts known regarding the production of the product abroad. Reports may be emailed to ICE.ForcedLabor@ice.dhs.gov.

ICE HSI Department of Motor Vehicles (DMV) Outreach was developed to raise awareness about corruption at DMV facilities. A principal component of the campaign is to alert DMV employees, law enforcement, and the public to the seriousness of fraud schemes perpetrated at DMV facilities. By adding education and outreach components, ICE HSI and its partners work together to deter the crime from happening, encourage people to report the crime, and ensure that their investigations are comprehensive and more efficient. Outreach materials, including posters, brochures, and short videos were developed by ICE HSI to support the outreach and are utilized by nearly every U.S. jurisdictional (state) and territorial DMV in employee new-hire and refresher ethics training. The materials provide guidance to DMV employees by promoting accountability and vigilance in an effort to reduce corruption and preserve the integrity of the DMV process. For more information, please email the Identity and Benefit Fraud Unit at ibfu-ice-hq@dhs.gov.

ICE HSI Forensic Laboratory (HSI-FL) provides a broad range of forensic, intelligence and investigative support to ICE HSI, DHS, and many other U.S. and foreign law enforcement agencies. The ICE HSI-FL is accredited by the American Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD/LAB). Forensic disciplines include questioned documents, fingerprints, and chemistry. Additionally, the ICE HSI-FL provides intelligence alerts, reference material on travel and identity documents, and fraudulent document detection training. The ICE HSI-FL manages the ICE HSI Polygraph Program and oversees the ICE HSI Evidence Recovery Team Program. For more information, visit www.ice.gov/hsi-fl.

ICE HSI International Operations Overseas Offices represent DHS' largest investigative law enforcement presence overseas. ICE HSI deploys more than 240 special agents and 156 Foreign Service nationals to 65 attaché offices in 46 countries in addition to liaison officers assigned to the 8 Department of Defense Combatant Commands. These agents enforce U.S. customs and immigration laws to protect the United States and its interests from terrorism and illicit trade, travel, and finance by conducting international law enforcement operations and removals.

The mission of ICE HSI International Operations is threefold: (1) Support domestic operations by conducting and coordinating investigations with foreign counterparts; (2) Disrupt transnational criminal organizations before they can bring illicit products, people, and proceeds into or out of the United States; (3) Build on international partnerships and to increase foreign capacity through outreach and training.

To locate and contact any of the ICE HSI International Offices, go to http://www.ice.gov/contact/hsi-international-ops.

You may also go through the ICE HSI domestic office in your jurisdiction or the 24/7 hotline at 866- 347-2423 (from U.S. and Canada) or 802-872-6199 (from any country in the world).

ICE HSI Tip Line is an internationally accessible venue through which the public, as well as federal, state, and local law enforcement agencies, can report suspected violations of ICE HSI-investigated immigration and customs laws. Special agents and intelligence research specialists assigned to the Tip Line take reports 24 hours, 365 days per year. and have the capability to customize questions to meet the needs of national enforcement priorities. Phone toll free 866-347-2423 from the U.S. and Canada, or from any country in the world phone 802- 372-6199. For more information, visit www.ice.gov/tips.

Human Rights Violators and War Crimes Center (HRVWCC) is a multi-agency program directed by ICE HSI with partners from the FBI, Department of State, USCIS and ICE's Human Rights Law Section. HRVWCC conducts investigations focused on human rights violations in an effort to prevent the United States from becoming a safe haven to those individuals who engage in the commission of war crimes, genocide, torture and other forms of serious human rights abuses from conflicts around the globe. Individuals seeking to report these abuses of human rights may contact the center at hrv.ice@dhs.gov. For additional information http://www.ice.gov/human-rights-violators-war-crimes-unit.

The Department of Homeland Security (DHS) Human Smuggling Cell (HSC) was established on October 1, 2014 in accordance with the White House National Security Council's mandate that law enforcement and the intelligence community collaborate and share intelligence and information regarding human smuggling. HSC will provide a means to operationalize intelligence in a timely manner to identify and disrupt human smuggling organizations. HSC is committed to a collaborative approach to detect, deter, disrupt and dismantle current human smuggling network activity, to include those organizations engaged in the movement of Central Americans and unaccompanied children to the United States. Defined by its function as a human smuggling targeting mechanism, the DHS/HSC will have access to the entire spectrum of human smuggling intelligence and will fuse this information into timely, operationalized intelligence products designed to enhance field enforcement efforts.

The International Organized Crime Intelligence and Operations Center (IOC-2) supports member agency efforts to disrupt and dismantle transnational criminal organizations (TCO) posing the greatest threat to the United States. This mission is accomplished through the deconfliction of member agency investigative endeavors; dissemination of leads and intelligence; coordination of multi-agency and multi-national law enforcement operations, investigations, prosecutions, and forfeiture proceedings; and the provision of operational funding. IOC-2 focuses primarily on TCOs involved in non-drug centric crime, such as money laundering, credit card fraud, weapons trafficking, identity theft, fraud scams, cybercrime, and human smuggling/trafficking. To facilitate its efforts, the IOC-2 leverages the resources of its ten member agencies, the OCDETF Fusion Center, the Special Operations Division, and other domestic and international resources. IOC-2 is limited to providing support to member agencies only; however, state and local law enforcement officers assigned to task forces operated by member agencies can utilize its capabilities.

National Bulk Cash Smuggling Center (BCSC) is a 24/7 operations and intelligence facility providing real-time tactical intelligence and investigative support to the federal, state, and local officers involved in enforcement and interdiction of bulk cash smuggling and the transportation of illicit proceeds. This is accomplished through the examination and exploitation of evidence obtained at our borders, during traffic interdictions, and other law enforcement encounters. The BCSC targets transnational criminal organizations who seek to avoid traditional financial institutions by repatriating illicit proceeds through an array of methods including commercial and private aircraft, passenger and commercial vehicles, maritime vessels, and pedestrian crossings at our U.S. land borders. For more information, visit https://www.ice.gov/bulk-cash-smuggling-center or contact BCSC@dhs.gov or 866-981-5332.

National Intellectual Property Rights Coordination Center (IPR Center) stands at the forefront of the U.S. government's response to global intellectual property theft and enforcement of its international trade laws. The IPR Center helps ensure national security by protecting the public's health and safety, the U.S. economy and U.S. warfighters by stopping predatory and unfair trade practices that threaten the global economy. The IPR Center is led by an ICE HSI director, along with deputy directors from ICE HSI, the Federal Bureau of Investigation (FBI) and CBP. The center brings together 23 partner agencies in a task force structure consisting of 19 key federal agencies, Interpol, Europol, and the governments of Canada and Mexico.

These task forces enable the IPR Center to leverage the resources, skills, and authorities of each partner, and they provide a comprehensive response to intellectual property theft. For additional information on available training opportunities, please contact the IPR Center at IPRCenter@dhs.gov. For more information on the IPR Center, visit http://www.iprcenter.gov/.

Operation Community Shield is the ICE HSI anti-gang initiative that combines ICE's expansive statutory and administrative enforcement authorities to combat the growth and proliferation of transnational criminal street gangs, prison gangs, and outlaw motorcycle gangs throughout the United States in cooperation with our federal, state, local, tribal, and foreign law enforcement partners. With our partners, ICE HSI enhances intelligence gathering and information sharing, exploits 21st century law enforcement technology, and capitalizes on our worldwide presence to combat these global criminal networks and mitigate the threats they pose to the public safety and national security of the United States and other countries. For more information, visit http://www.ice.gov/national-gang-unit.

The Organized Crime Drug Enforcement Task Force Fusion Center (OFC) fosters increased communication, cooperation, and coordination between member agencies through the provision of target deconfliction and direct intelligence support to ongoing HSI investigations. The OFC utilizes a consolidated database consisting of over 700 million law enforcement, regulatory, and immigration records to generate intelligence products for field exploitation. OFC is limited to providing support to member agencies only; however, state and local law enforcement officers assigned to task forces operated by member agencies can utilize its capabilities.

Parole and Law Enforcement Programs Unit (PLEPU) serves as the clearinghouse for all Significant Public Benefit Parole (SPBP) applications to ICE from federal, state, and local law enforcement agencies. SPBP is a mechanism that allows otherwise inadmissible aliens to come to the United States for law enforcement purposes.   For more information on the SPBP program, please call 800-973-2867.

Shadow Wolves. The ICE HSI Shadow Wolves are Native American Tactical Officers assigned to the Tohono O'odham Nation in Arizona to enforce immigration and customs laws and regulations. This reservation contains 2.8 million acres of land and includes a 75-mile-long stretch of the U.S. border with Mexico. The Shadow Wolves use their unique language and tracking skills to interdict and investigate contraband and have assisted law enforcement with the investigation of kidnappings, the deaths of illegal aliens, sexual assaults, missing children, and any reports of border violence. The Shadow Wolves have traveled to the Blackfeet Indian Reservation and the Bay Mills Chippewa Indian Reservation to share their expertise.

Additionally, the Shadow Wolves have conducted training with the U.S. Department of Defense in several of the former Soviet Republics to teach the ancient art of tracking to combat nuclear proliferation from the former Soviet Republics. For additional information, please contact 800-973-2867 and ask to speak with the Unit Chief for the ICE HSI Contraband Smuggling Unit in Washington, D.C. For more information, visit www.ice.gov/news/library/factsheets/shadow-wolves.htm.

Title 19 Cross-Designation. Title 19 of the U.S. Code section provides a mechanism for ICE HSI to designate federal, state, local, tribal, and foreign law enforcement officers as "Customs Officers." The unique resources and subject matter expertise of these officers complement ICE HSI investigations to effectively combat transnational crime. Law enforcement officers cross-designated under Title 19 U.S.C. § 1401(i) harness their invaluable experience with this unique federal authority to collectively enhance joint investigations of narcotics smuggling, money laundering, and fraud-related activities that disrupt and dismantle criminal organizations threatening this country's borders. With this authority, Title 19 cross-designated officers have the ability to execute and serve arrest warrants, subpoenas, and summonses in compliance with customs laws as well as carry firearms in compliance with ICE HSI firearms policy. For more information on the Title 19 Program Directive, please contact 800-973-2867 to speak with the Unit Chief for the ICE HSI Narcotics, Smuggling, and BEST Unit in Washington, D.C., or email the unit at HSITFO@ice.dhs.gov.   For additional information, visit www.ice.gov/customs-cross-designation.

Trade Transparency Unit (TTU) is a key component in ICE HSI's strategic efforts to combat and prevent Transnational Criminal Organizations (TCOs) from exploiting international trade and financial systems to disguise, move, and launder illicit funds and proceeds, a scheme commonly known as trade-based money laundering (TBML). The TTU uses ICE

HSI's unique authorities to access financial and international trade data to identify financial irregularities and international trade anomalies indicative of TBML, customs fraud, contraband smuggling and other financial crimes. For more information. visit www.ice.gov/trade-transparency.

Office of Intelligence and Analysis (I&A)

I&A is a member of the national Intelligence Community (IC) and ensures that information related to homeland security threats is collected, analyzed, and disseminated to the full spectrum of homeland security partners in the Department, at federal, state, local, tribal, and territorial levels, in the private sector, and in the IC.

I&A works closely with Department Component intelligence organizations as well as state, local, tribal, territorial, and private sector entities to ensure non-traditional streams of information are fused with traditional IC sources to provide a complete assessment of threats to the homeland.

The Under Secretary for Intelligence and Analysis, in the capacity of Chief Intelligence Officer for DHS, implements a mandate to integrate the Department's intelligence components and functions—the DHS IE—by driving a common intelligence mission.

I&A is the Executive Agent for coordinating federal support for state and major urban area fusion centers. It also leads the Department's information sharing efforts. I&A works to solidify productive and collaborative relationships with its partners to enhance information sharing. This collaboration and coordination is bolstered by the placement of I&A field personnel at state and major urban area fusion centers, as well as other strategic locations, providing direct intelligence support to key state, local, tribal, and territorial partners, and private sector partners. These services include engagement and intelligence and information sharing support, intelligence analysis, and intelligence collection and reporting.

Building Communities of Trust (BCOT). The BCOT initiative focuses on developing trust among law enforcement, fusion centers, and the communities they serve to address the challenges of crime and terrorism prevention. Since initial implementation, the BCOT initiative has been administered primarily by the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), a program that provides law enforcement with a capacity for gathering, documenting, processing, analyzing, and sharing suspicious activity reports about behaviors that have a potential nexus to terrorism. The NSI recognizes that each community has an important role in preventing crime and terrorism and uses the concept of community policing to build trust and cooperation to share information with state, local, tribal, and territorial law enforcement officers.

To help ensure that appropriate SAR reporting takes place, it is essential that law enforcement and community members have strong, trusting relationships. As these relationships are developed and maintained, members of the community are more likely to report crime and suspicious activities, which is why the NSI has worked with partners at the federal, state, and local levels—including U.S. Attorneys' Offices, privacy advocacy groups, faith leaders, and a diverse group of local community members—to implement the BCOT initiative.

The BCOT initiative has been implemented in over 15 urban areas across the country, with roundtables hosted by police chiefs, sheriffs' departments, and fusion centers through the support of U.S. Attorneys, Federal Bureau of Investigation field office executives, fusion center directors, and DHS field representatives.

Community leaders and local law enforcement share responsibility for addressing the prevention of crime and terrorism in their neighborhoods. BCOT roundtables provide a forum for community leaders and law enforcement officials to have a candid conversation on how to work together to keep communities safe from terrorism, crime, violence, and other locally-based problems that would be better

solved together. For more information, visit http://www.dhs.gov/publication/building-communities-trust-bcot-initiative, or contact your local Fusion Center.

Counterintelligence Fundamentals Workshop (CIFWS) is a training initiative offered by the DHS Counterintelligence Division (CIPD) to provide a one-day, on-site workshop to fusion centers as a means of promoting counterintelligence awareness to fusion centers personnel. The CIFWS program is intended to familiarize students with the potential intelligence collection threat directed against their facility, and state, local, tribal and territorial officials. This training also equips attendees with the ability to recognize an elicitation attempt or recruitment pitch. Prior to the training, CIPD notifies the I&A field representative assigned to the fusion center of training intent, potential training dates, and logistic requirements for this effort. I&A field representatives will be responsible for coordinating with their local FBI counterparts and promoting the event to their state, local, tribal and territorial counterparts; as well as to other DHS representatives.

DHS Open Source Enterprise Daily Intelligence Reports. These daily and weekly reports provide priority intelligence requirements on multiple topics of interest to facilitate a greater understanding of the nature and scope of threats and hazards to the homeland. They are provided to federal, state, local, tribal, territorial, and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures. These reports may be accessed via the Homeland Security Information Network (HSIN). To access or sign-up for HSIN, visit http://www.dhs.gov/homeland-security-information-network-hsin

DHS-Single Point of Service (DHS-SPS) serves as DHS Headquarter' central ingest point for receiving, tracking, and facilitating Operational and Intelligence Requests For Information (RFIs) to and from federal, state, local, tribal, and territorial partners. This process—undertaken by I&A and the Office of Operations Coordination and Planning—is not a replacement for existing lines of communication; rather, it serves as a resource to facilitate validated RFIs with an organization capable of providing a response. Before submitting an RFI to SPS, Federal and DHS Component partners should route their RFIs through their respective headquarters to ensure they have visibility. State and local partners should work through their Fusion Center(s) (via their deployed I&A Staff) to verify all local resources have been exhausted.
DHS-SPS representatives can be contacted at:

Open/STE: 202-282-9555
NSTS: 766-0888

NIPR: DHS-SPS-RFI@dhs.gov
HSDN: DHS-SPS-RFI@dhs.sgov.gov
JWICS: DHS-SPS-RFI@dhs.ic.gov.

Fusion Process Technical Assistance Program. Effective prevention efforts depend on the ability of all levels and sectors of government, as well as private industry, to collect, analyze, disseminate, and use homeland security and crime-related information and intelligence. Accordingly, the establishment of a network of fusion centers to facilitate effective nationwide information sharing has been a top priority. To assist in the development of this capability, the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ) partnered in 2007 to offer a series of fusion center technical assistance services. These services have been developed based on the input and guidance from the DHS

Office of Intelligence and Analysis (I&A); the Office of the Director of National Intelligence (ODNI); the Office of the Program Manager, Information Sharing Environment (PM-ISE); the Federal Bureau of Investigation (FBI); and experts from the state and local community—including the Global Justice Information Sharing Initiative (Global), the Criminal Intelligence Coordinating Council (CICC)—and will be delivered by subject-matter experts with experience in the development and operation of fusion centers. Fourteen services are offered to support the implementation of the *Fusion Center Guidelines,* the *Information Sharing Environment* (ISE) *Implementation Plan*, and the *Baseline Capabilities for State and Major Urban Area Fusion Centers* to facilitate the nationwide development and/or enhancement of the fusion process. To learn more or to apply for assistance please visit: https://ncirc.gov/.

HSDN Resources for State and Local Partners. Appropriately-cleared state and local personnel assigned to Fusion Centers are granted access to Secret-level network resources via the Homeland Secure Data Network (HSDN). These resources include intelligence products from I&A that are hosted on HSDN, as well as a range of other resources such as access to the National Counterterrorism Center Current portal for counter-terrorism information, the DEA portal for counternarcotics intelligence, and a number of Department of Defense sites including cybersecurity, counterterrorism, intelligence, and counternarcotics information.

The DHS Intelligence Training Academy (ITA) coordinates the design and delivery of entry, mid-level, and advanced intelligence training for I&A, the DHS Intelligence Enterprise (IE), and state, local, territorial, and tribal partners throughout the United States. The mission of the ITA is to advance students' knowledge, skills, and abilities through the creation and dissemination of homeland security intelligence training. The ITA is located in Washington, D.C. To obtain a copy of the ITA's course catalog or training calendar, please contact the IA-Registrar@hq.dhs.gov.

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). The NSI was established to facilitate fusion centers and law enforcement to easily share specific potential indicators of terrorist activity in order to prevent terrorist threats. The NSI training strategy is designed to increase the effectiveness of state, local, tribal, and territorial law enforcement and homeland security professionals in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to identify and prevent acts of terrorism. The NSI offers a host of customized online training for law enforcement and several other specific partner sectors. The training is designed to illustrate the importance of reporting suspicious activity linked to pre-operational behaviors that are indicative of terrorist activity, the attendant privacy protections, practical case examples and directions on how to report SAR. NSI resources and training may be accessed by visiting its website at https://nsi.ncirc.

National Protection and Programs Directorate (NPPD)

NPPD leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure.

BIOMETRIC IDENTITY MANAGEMENT

Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT). The IDENT system matches, stores, and shares fingerprints of more than 200 million unique identities for immigration, border management, law enforcement, credentialing, and national security purposes. IDENT is interoperable with the FBI's Next Generation Identification (NGI) system and provides state, local, tribal, and territorial law enforcement with access to IDENT information via NGI.

OBIM Biometric Support Center (BSC) provides expert fingerprint identification services in support of DHS's Automated Biometric Identification System, which contains the fingerprints of more than 200 million individuals. The BSC performs manual fingerprint comparisons to identify both known and unknown individuals (e.g. deceased subjects, cold cases). The BSC operates 24 hours a day/7 days a week. For additional information, contact afis@dhs.gov.

CHEMICAL SECURITY

Chemical Facility Anti-Terrorism Standards (CFATS). The CFATS program is the Department's regulatory program focused specifically on security at high-risk chemical facilities not located on navigable waterways. The program identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with these chemicals. DHS chemical security inspectors work in all 50 states to help ensure facilities have security measures in place to meet security risk-based performance standards.

For more information, visit http://www.dhs.gov/bombing-prevention-training. To request training, contact your local Protective Security Advisor (PSA) or contact OBP@hq.dhs.gov.

COUNTER-IMPROVISED EXPLOSIVE DEVICE (IED) PROGRAMS AND RESOURCES

Counter-IED & Risk Mitigation Courses and Resources. To reduce risk to the Nation's critical infrastructure, NPPD's Office for Bombing Prevention (OBP) develops and delivers a diverse curriculum of training to build nationwide counter-IED core capabilities and enhance awareness of terrorist threats. Coordinated through State Homeland Security Officials and training offices, courses educate federal, state, local, tribal, and territorial participants such as municipal officials and emergency managers, state and local law enforcement and other emergency services, critical infrastructure owners and operators, and security staff on strategies to prevent, protect against, respond to, and mitigate bombing incidents. Available courses are listed below. For more information, visit http://www.dhs.gov/bombing-prevention-training. To request training, contact your local Protective Security Advisor (PSA) or contact OBP@hq.dhs.gov.

- Bomb-making Materials Awareness Program (BMAP)
- Bomb Threat Management Workshop
- IED Counterterrorism Workshop
- IED Search Procedures Workshop
- Protective Measures Course
- Surveillance Detection Course for Law
- Enforcement and Security Professionals
- Vehicle Borne IED (VBIED) Detection Course

Counter-IED & Risk Mitigation Products. The following products are made available from OBP and can be found at http://www.dhs.gov/bombing-prevention-training.

- Counter-IED Awareness Cards & Posters
- DHS-DOJ Bomb Threat Guidance Brochure
- DHS Bomb Threat Procedures Checklist
- DHS-DOJ Bomb Threat Stand-off Card
- *FiRST* Smartphone Application
- Incident Management Preparedness and Coordination Toolkit (IMPACT)
- Protective Measures Guidance
- VBIED Identification Guide: Parked Vehicles
- Vehicle Inspection Guide (VIG) & Video

Multi-Jurisdiction Improvised Explosive Device Security Planning (MJIEDSP) program is a systematic process that fuses counter-IED capability analysis, training, and planning to enhance urban area IED prevention, protection, mitigation, and response capabilities. The MJIEDSP assists with collectively identifying roles, responsibilities, capability gaps, and how to optimize limited resources within a multi-jurisdictional planning area. OBP works closely with communities to provide expertise on planning and operational requirements for IED incident preparedness in alignment with the National Preparedness Goal and Core Capabilities. For more information, contact OBP@hq.dhs.gov.

National Counter-IED Capabilities Analysis Database (NCCAD) is an assessment program that uses a consistent and repeatable analytical methodology to assess and analyze the capabilities of bomb squads, explosives detection canine, dive, and SWAT teams throughout the United States. NCCAD assessments measure the capability elements of personnel, equipment, and training required for effective prevention, protection, and response to IED threats. This integrated information provides a snapshot of unit, State, regional and national counter-IED preparedness that informs decision makers on policy decisions, resource allocation for capability enhancement, and crisis management. For more information, contact OBP@hq.dhs.gov.

Technical Resource for Incident Prevention (TRIP*wire*) is the DHS 24/7 online, collaborative information-sharing network for bomb technicians, first responders, military personnel, government officials, intelligence analysts, and select private sector security professionals to increase awareness of evolving terrorist IED tactics, techniques, and procedures, as well as incident lessons learned and counter-IED preparedness information. Developed and maintained by OBP, the system combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist sources to help users anticipate, identify, and prevent IED incidents. TRIP*wire* is also regularly used to share critical information with our federal, state, local, tribal, territorial, and private sector security partners during periods of heightened alert or following IED related incidents. TRIPwire is available at no cost to registered subscribers at https://tripwire.dhs.gov, and features a public-access homepage with valuable preparedness information for the whole community. For additional information, contact OBP@hq.dhs.gov.

CYBERSECURITY

United States Computer Emergency Readiness Team (US-CERT) Portal is a web-based information sharing portal that enables members to exchange actionable cybersecurity information with other practitioners. The National Cybersecurity & Communications Integration Center's (NCCIC) operational branches, including US-CERT, share cyber threat indicators, alert, and warning information, and analytical findings through structured Portal compartments with registered public and private sector users, including state, local, tribal, and territorial government representatives. For more information and to request access, contact info@us-cert.gov.

The **Continuous Diagnostics and Mitigation (CDM) Program** enables federal, state, local, and tribal governments to obtain the risk-based, cost-effective tools and capabilities they need to fortify their IT systems and government networks. CDM allows system administrators to know the state of their respective network at any given time, and identify flaws for priority resolution at near-network speed, resulting in lower operational risk/exploitation.

DHS, in partnership with the General Services Administration (GSA), established a government-wide acquisition vehicle for CDM—the CDM Tools and Continuous Monitoring as a Service (CMaaS) blanket purchase agreement (BPA)—which is available to federal, state, local, and tribal government entities. BPA participants achieve cost savings through tiered-price and task order discounts, enabling more efficient use of financial resources.

State and local governments may use the Direct Order/Direct Bill option to procure products/services from the CDM BPA via the delegated procurement authority, GSA Federal Systems Integration and Management Center (FEDSIM). For specific ordering options, visit GSA's 2013 CDM/CMaaS Ordering Guide at www.gsa.gov/cdm.

For more information about CDM, visit:

- www.gsa.gov/cdm for ordering information
- www.us-cert.gov/cdm for operational information
- www.dhs.gov/cdm for the CDM public website

The CDM Program also offers a secure community of interest for stakeholders, hosted on the Homeland Security Information Network (HSIN). To request membership, email the CDM Program at cdm.fnr@hq.dhs.gov.

Cyber Resiliency Review (CRR) is an assessment that the Cyber Security Evaluation Program offers to measure and enhance the implementation of key cybersecurity capacities and capabilities of critical infrastructure. The purpose of the CRR is to gather information regarding cybersecurity performance from specific critical infrastructure in order to gain an understanding of the relationships and impacts of infrastructure performance in protecting critical infrastructure operations. The results can be used to evaluate a provider independent of other assessments, used with regional studies to build a common perspective on resiliency, and used to examine systems-of-systems (i.e., large and diverse operating and organizing models). The key goal of the CRR is to ensure that core process-based capabilities exist, are measureable, and are meaningful as predictors for an organization's ability to manage cyber risk to national critical infrastructure. For more information about the CRR, contact the CSEP program at CSE@dhs.gov.

Cybersecurity Evaluation Program (CSEP) conducts voluntary cybersecurity assessments across all 16 critical infrastructure sectors (including the Emergency Services Sector) and within state governments and large urban areas. CSEP affords critical infrastructure and key resources sector participants a portfolio of assessment tools, techniques, and analytics, ranging from those that can be self-applied to those that require expert facilitation or mentoring outreach. The CSEP works closely with internal and external stakeholders to measure key performances in cybersecurity management. The Cyber Resiliency Review is being deployed across all 16 critical infrastructure sectors, state, local, tribal, and territorial governments. For more information, visit www.us-cert.gov/ccubedvp/self-service-crr or contact CSE@dhs.gov.

Cybersecurity Information Products provide current cybersecurity information and recommended security practices to help users understand cybersecurity issues and mitigation options. This information enables users to reduce their exposure and susceptibility to cyber-attacks and exploits. For a complete list and access to cybersecurity information products, visit https://www.us-cert.gov/security-publications and http://ics-cert.us-cert.gov/Information-Products.

Emergency Services Sector-Cyber Risk Assessment (ESS-CRA). The 2012 ESS-CRA is the first ESS-wide cyber risk assessment that analyzes strategic cyber risks to ESS infrastructure. The ESS-CRA process provides a national-level risk profile that ESS partners can use to prioritize how they spend resources and where to focus training, education, equipment investments, grant requests, and further study. The risk assessment consisted of seven evaluation sessions to solicit input from ESS subject-matter experts. Each scenario evaluated threats, vulnerabilities, and consequences to ESS cyber infrastructure. Stakeholders chose scenarios based on what would have the widest impact - the scenarios likely to affect the most disciplines at a time. The final ESS-CRA report includes a risk profile showing how the scenarios would affect each discipline, and the operational impact. Cyber risks to each discipline are ranked from high to low in terms of likelihood and consequence. The assessment approach is not intended to be guidance for individual entity's risk management activities. Instead, by increasing the awareness of risks across the public and private sector domains, the ESS-CRA serves as a foundation for ongoing national-level collaboration to enhance the security and resilience of the ESS disciplines. If you have any questions about the ESS Cyber Risk Assessment, please contact ESSTeam@hq.dhs.gov.

Enhanced Cybersecurity Services (ECS) is an intrusion prevention capability that helps U.S. based organizations (including state, local, tribal, and territorial government groups) protect their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sharing sensitive and classified cyber threat information with accredited Commercial Service Providers (CSPs). These CSPs in turn use that information to block certain types of malicious traffic from entering customer networks. Groups interested in receiving ECS services should visit http://www.dhs.gov/enhanced-cybersecurity-services for more information.

Federal Virtual Training Environment (FedVTE) is an online training center featuring a wide range of cybersecurity courses – to state, local, tribal, and territorial government employees across the country. FedVTE provides government-wide, on-demand access to cybersecurity training to help the workforce maintain expertise and foster operational readiness at no cost to users. Courses range from beginner to advanced levels and is accessible from any internet-enabled computer. For more information, visit the National Initiative for Cybersecurity Careers and Studies portal at: http://niccs.us-cert.gov/training/fedvte.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The ICS-CERT focuses on control system security across all critical infrastructure and key resource sectors. The ICS-CERT supports asset owners with reducing the risk of cyber-attacks by conducting outreach for awareness, performing assessments, providing alerts and advisories, conducting incident response activities, and performing technical analysis of malware, artifacts, and vulnerabilities. For more information, visit http://www.ics-cert.us-cert.gov or contact ICS-CERT at ics-cert@hq.dhs.gov.

If an organization believes it is experiencing a cyber event on control systems/critical infrastructure please call 1-877-776-7585 or e-mail ICS-CERT at ics-cert@hq.dhs.gov. To report ICS software vulnerability visit www.kb.cert.org/vuls/html/report-a-vulnerability/ and fill out the Vulnerability Reporting Form. Please follow the directions to encrypt to the CERT Pretty Good Privacy key in order to protect sensitive, non-public vulnerability information.

Industrial Control System Cybersecurity Standards and References provide an extensive collection of cybersecurity standards and reference materials as a ready resource for the industrial control system stakeholder community. The collection provides a one-stop location for accessing papers, reports, references, and standards associated with industrial control system cybersecurity. To view the collection, visit http://ics-cert.us-cert.gov/Standards-and-References. For more information, contact ics-cert@dhq.dhs.gov.

Industrial Control Systems Cybersecurity Training. ICS-CERT performs outreach activities and assists the control systems community to improve their cybersecurity preparedness through various cybersecurity training courses. For more information, visit http://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT.

Information Technology Government Coordinating Council provides a forum for interagency coordination, and partnership among DHS, National Cyber Security Division, federal, state, local, tribal, and territorial governments with a role in protecting the IT Sector. For more information, visit www.dhs.gov/information-technology-sector.

Information Technology Sector Risk Assessment provides an all-hazards risk profile that public and private IT Sector partners can use to inform resource allocation for research and development and other protective measures which enhance the security and resiliency of the critical IT Sector functions. For more information, visit www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf or contact ncsd_cips@hq.dhs.gov.

Multi-State Information Sharing and Analysis Center (MS-ISAC) seeks to improve the overall cybersecurity posture of state, local, tribal, and territorial partners. Collaboration and information sharing among members, private sector partners, and DHS are the keys to success. State, local, tribal, and territorial government representatives who believe they are experiencing a cyber event of any kind, please call 1-866-787-4722 for the 24x7 MS-ISAC Security Operations Center, or visit http://msisac.cisecurity.org/about/incidents and click on the "Report an Incident" button.

National Coordinating Center for Communications (NCC) continuously monitors national and international incidents and events that may impact national security and emergency preparedness communications. Incidents include not only acts of terrorism, but also natural events such as tornadoes, floods, hurricanes, and earthquakes. To receive information on the NCC or to be added to the NCC distribution list, please contact the NCC Watch at 703-235-5080 or e-mail NCC@hq.dhs.gov.

National Cybersecurity & Communications Integration Center (NCCIC) serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities. The center's activities include providing greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation, and recovery actions. Stakeholders can report cybersecurity incidents (including unexplained network failures), the discovery of malicious code, and vulnerability information at https://forms.us-cert.gov/report. Contact the NCCIC Operations Center at NCCIC@us-cert.gov or 888-282-0870.

National Cybersecurity Assessment and Technical Services Team (NCATS). The National Cybersecurity Assessment and Technical Services (NCATS) team supports the NCCIC mission by offering cybersecurity scanning and testing services that identify vulnerabilities within stakeholder networks and provide risk analysis reports with actionable remediation recommendations. These critical services enable proactive mitigation to exploitable risks and include network (wired and wireless) mapping and system characterization, vulnerability scanning and validation, threat identification and evaluation, social engineering, application, database, and operating system configuration review, and incident response testing.
To learn more about NCATS or request information about their services, please contact NCATS_INFO@HQ.DHS.GOV.

National Cyber Exercise and Planning Program (NCEPP) increases the cyber preparedness and resilience of the nation through the conduct and development of cyber exercises and planning templates for and with public, private, and international stakeholders. As part of the NCCIC, NCEPP works with state, local, tribal, and territorial partners to provide direct cyber exercise support as a service or through participation in the Department's flagship biennial national-level cyber exercise series: "Cyber Storm." Additionally, NCEPP works with a range of stakeholders to develop and deliver planning templates, such as the Cyber Capabilities Framework and state, local, tribal, and territorial Cyber Incident Annex Template. NCEPP's cyber planning and exercise offerings are available at no cost to the state, local, tribal, and territorial community. For additional information, contact CEP@hq.dhs.gov.

National Cyber Security Awareness Month (NCSAM) is an annual campaign held each October to raise awareness about cyber security among all Americans, with law enforcement across the country participating. National Cyber Security Awareness Month, the capstone event of the Stop.Think.Connect. Campaign, is designed to engage and educate public and private sector partners through events and initiatives with the goal of raising awareness about cybersecurity and increasing the resiliency of the nation in the event of a cyber incident. To learn more about NCSAM and find out how to get involved, please contact the Campaign at stopthinkconnect@dhs.gov or visit www.dhs.gov/national-cyber-security-awareness-month.

State, Local, Tribal and Territorial Cybersecurity Engagement Program fosters the relationships that protect our Nation's critical infrastructure and facilitates access to no-cost programs, resources, and services for state, local, tribal, and territorial governments. Governors and other appointed and elected state, local, tribal, and territorial government officials receive cybersecurity risk briefings and information on available resources. More importantly, these officials look to the program to identify cybersecurity initiatives and partnership opportunities with federal agencies, as well as state and local associations, that will help protect their citizens online. For more information on the State, Local, Tribal, and Territorial Cybersecurity Engagement Program, contact SLTTCyber@hq.dhs.gov.

The **Fusion Center Cyber Pilot** was a one-year pilot for developing a framework for all fusion centers on how to integrate cyber security into their areas of responsibility. Under the guidance of a multi-agency review board, the DHS, the MS-ISAC, and others worked with six Fusion Centers to develop the resulting *Cyber Integration for Fusion Centers, An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers*. This document is accompanied by a Cyber Toolkit for fusion centers to use in building or improving their cyber programs. For more information, please contact SLTTCyber@hq.dhs.gov.

Stop.Think.Connect.™ Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Initiated by President Obama's Cyberspace Policy Review, DHS leads the Campaign in partnership with the National Cyber Security Alliance and the Anti-Phishing Working Group. Law enforcement agencies and other organizations can receive free cybersecurity materials (including tip sheets, presentations, and more) and collaborate with other members, including the Internatioanl Association of Chiefs of Police and the Department of Justice, by joining the Cyber Awareness Coalition of government agencies or the National Network of non-profit groups. For more information visit www.dhs.gov/stopthinkconnect. or contact the Campaign at stopthinkconnect@dhs.gov.

United States Computer Emergency Readiness Team (US-CERT) responds to major incidents, analyzes threats and exchanges critical cybersecurity information with trusted

partners around the world. US-CERT is working more closely than ever with partners to develop a comprehensive picture of malicious activity and mitigation options.
In its role as the federal information security incident center, US-CERT accepts incident notifications 24x7x365. Guidance for federal and non-federal entities to use when submitting an incident notification can be found at https://www.us-cert.gov/incident-notification-guidelines. To report an incident, malware, phishing or vulnerabilities, visit https://www.us-cert.gov/forms/report.

US-CERT shares actionable information through its public-facing website, secure portal, and National Cyber Awareness System. Learn more about US-CERT's products and services at https://www.us-cert.gov/ and by contacting 888-282-0870 or info@us-cert.gov.

US-CERT National Cyber Awareness System (NCAS) offers subscriptions to a variety of cybersecurity information for users with varied technical expertise. NCAS products include Alerts, Bulletins, Tips and Current Activity updates. A subscription to any or all NCAS products ensures access to timely information about security topics and threats. To learn more or subscribe, visit https://www.us-cert.gov/mailing-lists-and-feeds. This page includes information about how to use US-CERT's syndicated feeds. For additional information, contact info@us-cert.gov.

Vulnerability Notes Database and National Vulnerability Database (NVD) provide timely information about software vulnerabilities, including associated impact, solutions and workarounds, and lists of affected vendors.
For more information, visit www.kb.cert.org/vuls, http://web.nvd.nist.gov/view/vuln/search, contact info@us-cert.gov or call 888-282-0870.

The **Critical Infrastrucure Cyber Community (C³) Voluntary Program** (pronounced "C-Cubed") is a public-private partnership aligning business enterprises as well as federal, state, local, tribal, and territorial governments to existing resources that will assist their efforts to use the National Institute of Standards and Technology (NIST) Cybersecurity Framework to manage their cyber risks as part of an all-hazards approach to enterprise risk management. For more information, visit www.us-cert.gov/ccubedvp.

FEDERAL PROTECTIVE SERVICE RESOURCES

The Federal Protective Service (FPS) protects federal facilities and their occupants and visitors by providing law enforcement and protective security services, leveraging the intelligence and information resources of our network of federal, state, local, tribal, territorial and private sector partners. FPS provides security planning; stakeholder engagement; law enforcement and information sharing services; and incident response.

Explosive Detector Canine (EDC) Program is a critical element of FPS's comprehensive security measures and supports strategic detection activities to clear identified areas of interest of explosive threats. The EDC teams provide mobile and effective capabilities for the protection of life and property through the provision of a strong, visible, and psychological deterrence against criminal and terrorist threats. EDC teams are the most effective countermeasure available today for detection of explosives. The EDC teams, each comprised of a dog and a handler with law enforcement authority, conduct searches for a variety of explosive materials on or near building exteriors, parking lots, office areas, vehicles, materials, packages and persons in and around federal facilities. They also provide immediate and specialized response to bomb threats and unattended packages or other such dangerous items that may present a hazard to a federal facility. For more information contact the Chief of the Canine Operations Branch Uniformed Operations Division at 703-235-6080 or John.Hogan1@dhs.gov.

Mobile Command Vehicle (MCV) Program supports FPS's mission through the provision of mobile, on-site platforms for command, control, and communications during terrorist attacks, natural disasters, National Special Security Events, and other similar occurrences. The MCVs can rapidly deploy to any location in the continental U.S. where the communications infrastructure is inadequate or has been disrupted, or where enhanced interoperability among law enforcement agencies is needed. Incident management in the nation's current threat environment requires mobility, interoperability among public safety agencies, reliability, and cost effectiveness. FPS MCVs meet this need. MCVs can support daily operations as well as special deployments of the FPS Crisis Response Teams and other organizational elements. These highly specialized vehicles augment the capabilities of the FPS dispatch and call centers, known as MegaCenters, by allowing them to remotely dispatch units and link different radio systems together without the need to actually send personnel to the scene. Each MCV also provides an environmentally controlled platform for on-scene command and control functions, with small conferencing areas, video-teleconferencing, data analysis and processing, and information acquisition and management for situational awareness and common operating picture development.

FPS has eight MCVs located at regional offices around the country, as well as four SUV-based mobile communications vehicles, known as "Rabbits." The Rabbits provide most of the same communications capabilities as the MCVs, but lack the command and control space and workstations. The Rabbits afford a rapid deployment capability, as well as the ability to navigate tight spaces and unimproved roads, which allows for the projection of communications services into areas that would otherwise be inaccessible. The Rabbits are designed to extend their electronic footprint into buildings of opportunity so that they can be rapidly converted into command posts with the full communications services. Strategic locations around the country ensure that each vehicle has a 750 mile "first due" response radius and that any area of the continental U.S. can be provided with service within one day. For more information, contact the Chief of the Critical Incident Management Branch, Uniformed Operations Division at 703-235-6080 or Robert.Scott4@dhs.gov.

INFRASTRUCTURE SECURITY AND RESILIENCE TRAINING AND RESOURCES

Critical Infrastructure Security and Resilience Training includes web-based independent study and classroom training and materials that address a variety of topics relevant to law enforcement that are designed to promote the knowledge and skills needed to implement critical infrastructure protection, and resilience activities. The Independent Study courses developed by the Office of Infrastructure Protection are available free of charge through the FEMA Emergency Management Institute. More information about infrastructure protection training programs is available at www.dhs.gov/video/training-programs-infrastructure-partners.

- *Critical Infrastructure Protection: Achieving Results through Partnership and Collaboration* (IS-913) provides an overview of the elements and processes that develop and sustain successful critical infrastructure protection partnerships and collaborations. For more information, visit http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?CODE=IS-913.a.

- *Implementing Critical Infrastructure Protection Programs (IS-921.a)* addresses processes for informing partnerships, sharing information, managing risk, and ensuring continuous improvement. For more information, visit https://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-921.a

- *Active Shooter: What You Can Do (IS-907)*, which uses interactive scenarios and videos to illustrate how individuals who become involved in an active shooter situation should react. For more information, visit http://training.fema.gov/EMIWeb/IS/IS907.asp.

- *Critical Infrastructure Security: Theft and Diversion – What You Can Do* (IS-916) is designed for critical infrastructure employees and stakeholders, and provides information and resources available to identify threats and vulnerabilities to critical infrastructure from theft and diversion of critical resources, raw materials, and products that can be used for criminal or terrorist activities. The course also identifies actions that can be taken to reduce or prevent theft and diversion. For more information, visit http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-916.

- *Protecting Critical Infrastructure Against Insider Threats (IS-915)* provides guidance to critical infrastructure employees and service providers on how to identify and take action against insider threats to critical infrastructure. It is designed for all personnel and service providers who are associated with critical infrastructure. For more information, visit http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-915.

- *Retail Security Awareness: Understanding the Hidden Hazards (IS-912)*, which is designed to make persons involved in commercial retail operations aware of the actions they can take to identify and report suspicious purchases or thefts of products that actors could use in terrorist or other criminal activities. For more information, visit http://training.fema.gov/EMIWeb/IS/IS912.asp.

- *Surveillance Awareness: What You Can Do* (IS-914) provides training on actions that can be taken to detect, deter, and report suspicious activities associated with adversarial surveillance. It is designed for individuals with little to no physical or operations security experience. For more information, visit http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-914.

- *Workplace Security Awareness (IS-906)* which provides training for a broad audience recognizing threats and improving security in the workplace. For more information, visit http://training.fema.gov/EMIWeb/IS/IS906.asp.

These courses can be used by law enforcement to educate members of their community. The Workplace Security and Active Shooter courses are supplemented by classroom materials (instructor guides, student manuals, and visuals) that can be downloaded from the website.

Homeland Security Information Network – Critical Infrastructure (HSIN-CI)

HSIN-CI provides secure networked information sharing covering the full range of critical infrastructure interests. Validated critical infrastructure partners are eligible for HSIN-CI access.

The National Infrastructure Coordinating Center (NICC) posts content from a variety of internal and external sources that is available to all critical infrastructure partners, including incident situation reports, threat reports, impact modeling and analysis, common vulnerabilities, potential indicators, and protective measures.

The NICC combines current high-interest incidents and events on the HSIN-CI "front page" to enable easy access to relevant information.

Individual sectors and sub-sectors self-manage more specific portals within HSIN-CI where smaller communities of participants receive and share relevant information for their particular information needs.

HSIN-CI also includes capabilities to facilitate multiple types of information sharing and coordination, including suspicious activity reporting, webinars, shared calendars, etc.

To ensure broad sharing of essential information, the NICC also receives and provides information via other HSIN portals.

To request HSIN-CI access, submit the following to HSIN.Helpdesk@hq.dhs.gov:

- Name
- Employer
- Title
- Business email
- Brief written justification

For questions regarding HSIN-CI access, please contact the NICC.

Infrastructure Protection Gateway (IP Gateway) serves as the single interface through which DHS mission partners can access a large range of integrated IP tools and data to conduct comprehensive vulnerability assessments and data analysis. This, in turn, enables homeland security partners to quickly identify relevant vulnerability and consequence data in support of event planning and response efforts. The IP Gateway provides various data collection, analysis, and response tools into one system, streamlining access to IP's tools and datasets by leveraging a single user registration, management, and authentication process. Highlights of the IP Gateway include the ability to access:

- a selection of physical and cyber vulnerability tools and security surveys;
- a consolidated library of critical infrastructure data, assessments and reports;
- integrated data visualization and mapping tools to support complex data analysis; and
- situational awareness tools to support special event and incident planning and response activities.

For more information, contact IPGateway@hq.dhs.gov or 1-866-844-8163.

National Infrastructure Coordinating Center (NICC). The NICC serves as a clearinghouse to receive and synthesize critical infrastructure information and provide that information back to decision makers at all levels inside and outside of government to enable rapid, informed decisions in steady state, heightened alert, and during incident response. The NICC serves as the national focal point for critical infrastructure partners to obtain situational awareness and integrated actionable information to protect physical critical infrastructure. The mission of the NICC is to provide 24/7 situational awareness, information sharing, and unity of effort to ensure the protection and resilience of the Nation's critical infrastructure. When an incident or event impacting critical infrastructure occurs that requires coordination between DHS and the owners and operators of critical infrastructure, the NICC serves as a national coordination hub to support the protection and resilience of physical critical infrastructure assets. Establishing and maintaining relationships with critical infrastructure partners both within and outside the Federal Government is at the core of the NICC's ability to execute its functions. The NICC collaborates with federal departments and agencies and private sector partners to monitor potential, developing, and current regional and national operations of the Nation's critical infrastructure sectors. For more information, contact nicc@hq.dhs.gov or 202–282–9201.

Office of Cyber and Infrastructure Analysis (OCIA) provides infrastructure consequence analysis and prioritization capabilities to DHS, government, and private sector stakeholders. OCIA experts analyze the effects of risk mitigation actions in many forms, including strategic threat and risk analysis; modeling and simulation; and analytic support to Department decision makers and security partners before, during, and after incidents.

OCIA, the Office of Intelligence and Analysis, and FEMA also provides risk analysis tradecraft training to Fusion Centers. For access to risk analysis training call 202-282-8866 or e-mail FusionCenterSupport@hq.dhs.gov. For questions or requests, contact OCIA@hq.dhs.gov.

Protected Critical Infrastructure Information (PCII) Program
Are you finding it difficult to obtain the vital critical infrastructure information (CII) needed to support your critical infrastructure initiatives? Are private industry partners reluctant to share their data with you, out of fear that it could expose potentially sensitive and/or proprietary information to the public?

If so, the PCII Program offers a way for homeland security analysts to access vital CII, while offering assurances to facility owners/operators that their information is protected from public disclosure. Created by Congress in the Critical Infrastructure Information Act of 2002, the PCII Program ensures that PCII in the government's hands is protected from disclosure, from use in civil litigation; or for regulatory purposes.

By integrating PCII protections into the data-collection process, homeland security analysts are better positioned to obtain and protect the critical business sensitive information needed to assess and understand the risk landscape, and provide leading indicators for emerging cyber security threats, and vulnerabilities to critical infrastructure.

To find out how the PCII Program can support your programmatic needs, contact us at pcii-assist@dhs.gov or at 1-866-844-8163.

Protective Security Advisors (PSAs) are security subject matter experts who engage on protective measures and resilience planning with state, local, tribal, and territorial government mission partners and members of the private sector stakeholder community to protect the Nation's critical infrastructure. As part of their mission supporting critical infrastructure protection, the PSAs plan, coordinate, and conduct security surveys and assessments; plan and conduct assistance visits; support National Special Security Events and Special Event Activity Rating events; respond to incidents; and plan, coordinate, and conduct training – to include coordinate improvised explosive device (IED) awareness and IED risk mitigation training. For more information or to contact your local PSA, contact PSCDOperations@hq.dhs.gov.

PUBLIC SAFETY AND EMERGENCY COMMUNICATIONS

All-Hazards Communications Unit Leader (COML) Course is an NPPD's Office of Emergency Communications (OEC) Technical Assistance course that familiarizes communications professionals with the role and responsibilities of a COML under the National Incident Management System Incident Command System (NIMS ICS) and provides exercises that reinforce the lecture materials. OEC offers this course jointly with FEMA/EMI, as "E-969, NIMS ICS All Hazards Communications Unit Leader." This course is available to state and local law enforcement agencies as part of OEC Technical Assistance. For more information, contact oec@hq.dhs.gov.

All-Hazards Communications Unit Technician (COMT) Course introduces public safety professionals and support staff to various communications concepts and technologies including interoperable communications solutions, land mobile radio (LMR) communications, satellite, telephone, data and computer technologies during an incident response and for planned events. The course is taught by OEC/ICTAP instructors who have both practitioner and Communications Unit experience and is designed for state, territory, tribal and urban emergency response personnel in all disciplines who have a technical communications background. For more information, contact oec@hq.dhs.gov.

Auxiliary Communications workshop is designed for the Auxiliary Communicator and volunteer who provide emergency backup radio communications support to public safety agencies for planned or unplanned events at state and local levels. It is designed for amateur radio operators or groups who work with public safety and cross-disciplinary emergency response professionals. This workshop is available to state and local public safety personnel as part of OEC's Technical Assistance Program. For more information, contact oec@hq.dhs.gov.

Emergency Communications Guidance Documents and Methodologies are stakeholder-driven guidance documents and methodologies to support emergency responders across the Nation as they plan for and implement emergency communications initiatives. These resources identify and promote best practices for improving statewide governance, developing standard operating procedures, managing technology, supporting training and exercises, and encouraging use of interoperable communications. Each is available publicly and is updated as needed. Examples include the Public Safety Communications Evolution Brochure, Establishing Governance to Achieve Statewide Communications Interoperability, and the Formal Agreement and Standard Operating Procedure Template Suite. For more information, contact oec@hq.dhs.gov or visit www.publicsafetytools.info.

National Emergency Communications Plan (NECP) sets goals and identifies key national priorities to enhance governance, planning, technology, and training and exercises to improve disaster communications capabilities. Originally published in 2008, the NECP was revised in 2014 to address the rapidly evolving emergency communications landscape, specifically the increased adoption of IP-based technologies. While the 2014 NECP continues to focus on the maintenance and operation of Land Mobile Radio (LMR) systems, it urges state and local jurisdictions to plan and prepare for the adoption and integration of broadband technology into emergency communications, including the Nationwide Public Safety Broadband Network (NPSBN). Continued collaboration between public and private sector entities is vital as the 2014 NECP begins to be implemented nationwide. For more information, visit www.dhs.gov/necp or contact OECNECP@hq.dhs.gov.

OEC Interoperable Communications Technical Assistance (TA) Program provides technical assistance at no cost to all levels of state, local, and tribal law enforcement to support interoperable communications solutions and practices. This assistance is offered annually through Statewide Interoperability Coordinators (SWICs) based on risk and capabilities, and it supports all lanes of the SAFECOM Interoperability Continuum. There are 72 TA services are offered through the OEC TA Catalog that can be viewed on the PSTools site at: www.publicsafetytools.info. These offerings are at no-cost and can be requested through Statewide Interoperability Coordinators. The services provided range from communications-focused exercises, NIMS ICS communications training to developments in broadband for public safety, dispatch operations and NG9-1-1-implementation. For more information, contact oec@hq.dhs.gov.

OEC Route Diversity Project (RDP) assists agencies on increasing the continuity of their local access networks. The local access network is the "last mile" connection between an agency's on-site communications infrastructure and the service provider's Central Office (CO) or Point of Presence (POP). In the event of an undesirable event, such as a cable cut, flood, or damage to the service provider's facility, the local access network may be entirely lost, leaving the agency unable to perform mission-essential functions. The RDP methodologies, tools, and handbooks are designed to assist agencies evaluate their organization's connectivity and suggest mitigation solutions to increase route diversity. For more information, contact oec@hq.dhs.gov.

Priority Telecommunications Services (PTS) programs provide national security and emergency preparedness (NS/EP), public safety and first responders, and Critical Infrastructure Key Resources (CIKR) industries the ability to communicate on telecommunications networks during times of congestion. This is accomplished through the following three services:

- **Government Emergency Telecommunications Service** (GETS) provides priority access to the landline networks when abnormal call volumes exist, providing enhanced call completion for critical personnel.
- **Wireless Priority Service** (WPS) provides priority voice access to the cellular networks when abnormal call volumes exist, providing enhanced call completion for critical public safety personnel. An initiation fee and nominal monthly cost are associated with this service through your selected telecommunications carrier.
- **Telecommunications Service Priority** (TSP) provides priority repair and installation of critical voice and data circuits in many situations. An initiation fee and nominal monthly cost are associated with this service.

For more information, please visit the following websites: www.dhs.gov/gets; www.dhs.gov/wps; www.dhs.gov/tsp.

The SAFECOM Program works to improve multi-jurisdictional and intergovernmental communications interoperability. Its membership includes more than 70 members representing state, local, and tribal emergency responders, and major intergovernmental and national public safety associations, who provide input on the challenges, needs, and best practices involving emergency communications. The SAFECOM website provides members of the emergency response community and other constituents with information and resources to help them meet their communications and interoperability needs. For more information, visit www.safecomprogram.gov, or contact SAFECOMGovernance@dhs.gov.

SAFECOM Guidance on Emergency Communications Grants provides recommendations to grantees seeking funding for interoperable emergency communications projects, including allowable costs, items to consider when funding emergency communications projects, grants management best practices for emergency communications grants, and information on standards that ensure greater interoperability. The guidance is intended to ensure that Federally-funded investments are compatible and support national goals and objectives for improving interoperability nationwide. For more information visit www.safecomprogram.gov/grant/Default.aspx or contact oec@hq.dhs.gov.

The Southwest Border Communications Working Group (SWBCWG) serves as a forum for federal, state, local, and tribal agencies in Arizona, California, New Mexico, and Texas to share information on common issues, collaborate on existing and planned activities, and facilitate federal involvement in multi-agency projects within the Southwest Border Region. The SWBCWG aims to enhance communications operability and interoperability, effectively use the region's available critical communications infrastructure resources, and ensure that programs continue to meet the stakeholders' needs. For more information, contact oec@dhs.gov.

Statewide Communication Interoperability Plans (SCIPs) are locally-driven, multi-jurisdictional, and multi-disciplinary statewide strategic plans to enhance emergency communications. The SCIP provides strategic direction and alignment for those responsible for interoperable communications at the state, regional, local, and tribal levels. These strategic plans outline and define the current and future vision for communications interoperability within the state or territory. They also align emergency response agencies with the goals, objectives, and initiatives for achieving that vision. SCIPs are living documents that are typically updated on an annual basis, or as frequently as needed. For more information, visit www.dhs.gov/statewide-communication-interoperability-plans.

DHS Privacy Office (PRIV)

PRIV protects all individuals regardless of citizenship by embedding and enforcing privacy protections and transparency in all DHS activities. PRIV works with every DHS component and program to ensure that privacy considerations are addressed when planning or updating any program, system, or initiative.

PRIV uses the DHS Fair Information Practice Principles as the policy framework to enhance privacy protections by assessing the nature and purpose for all personally identifiable information (PII) collected to fulfill the Department's mission.

PRIV makes much of its work publically accessible via www.dhs.gov/privacy to share its experience and work products with DHS's partners and the public.

PRIV is always available to support our state and local partners. Please feel free to contact us at 202-343-1717 or privacy@dhs.gov.

The following materials may be of particular interest to state and local law enforcement offices, programs, and IT systems.

Privacy Compliance Reviews. PRIV issues privacy policies and conducts Privacy Impact Assessments (PIAs) to implement those policies. Later, PRIV revisits the results of these efforts to evaluate performance according to its guidance principles and standards. For more information, visit www.dhs.gov/privacy-investigations-compliance-reviews.

Privacy Compliance program, guidance, and templates. PRIV operates a robust privacy compliance program, using the PIA and other tools to assess and document the integration of rules into the Department's programs and IT systems. To foster public trust through transparency, DHS publishes its PIAs, as well as the templates and guides used to create those PIAs, directly to the public. For more information, visit www.dhs.gov/privacy-compliance.

Policy Establishing the Fair Information Practice Principles as a matter of Department procedure. DHS believes in a set of privacy principles that guide all DHS strategies, programs, and IT systems. DHS uses these principles as the foundation for new initiatives and PIAs of existing programs. DHS memorialized these principles as department policy. For more information, visit www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

Policy Establishing the Privacy Impact Assessment as a standardized government privacy compliance process. PRIV uses a structured approach to build privacy protections into specific programs: The PIA. DHS formally established the PIA requirement as a matter of policy. For more information, visit www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf.

Privacy Incident Handling Guidance. All organizations face the risk of privacy breaches and other incidents. PRIV created a formal approach to preparing for and responding to privacy incidents. For more information, visit www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.

Privacy Outreach & Education. PRIV shares its experience directly with the public and its partners in the public, private, and academic sectors. For more information, visit www.dhs.gov/privacy-events.

PRIV issues tailored educational materials to support its government and commercial colleagues, for example: The Handbook for Safeguarding Sensitive Personally Identifiable Information. For more information, visit www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf.

Science and Technology Directorate (S&T)

The S&T Directorate's mission is to improve homeland security by providing to customers state-of-the-art technology that helps them achieve their missions. S&T customers include the operating components of the Department, and state, local, tribal, and territorial emergency responders and officials.

The **Centers of Excellence (COE)** network is an extended consortium of hundreds of universities generating ground-breaking ideas for new technologies and critical knowledge, while also relying on each other's capabilities to serve the Department's many mission needs.

Managed through S&T's Office of University Programs, the COEs organize leading experts and researchers to conduct multidisciplinary homeland security research and education. All COEs work closely with academia, industry, Department components, and first-responders to develop customer-driven research solutions to 'on the ground' challenges as well as provide essential training to the next generation of homeland security experts.

Each center is university-led or co-led in collaboration with partners from other institutions, agencies, national laboratories, think tanks and the private sector. The research portfolio is a mix of applied research addressing both short and long-term needs. The COE extended network is also available for rapid response efforts. For more information, visit www.dhs.gov/science-and-technology/centers-excellence.

The **First Responders Group** is S&T's component that works directly with first responder organizations to identify and prioritize gaps in capabilities, establish operational requirements and standards, and develop and commercialize solutions. Projects in the First Responders Group's four strategic priority areas – communications, data sharing, first responder safety and effectiveness, and radiological/nuclear response and recovery research and development – result directly from close collaboration with the end users. Reflecting S&T's focus on transition, FRG has worked to ensure that technologies developed in coordination with S&T are available to first responder communities nationwide; S&T's technologies are included in the Federal Emergency Management Agency's Authorized Equipment List that public safety agencies are authorized to purchase from with their federal grant dollars. For more information, visit www.dhs.gov/science-and-technology/first-responders.

FirstResponder.gov is a website that enables federal, state, local, tribal, and territorial first responders to easily access and leverage federal resources on products, standards, testing and evaluation, and best practices to develop or deploy technologies to enhance homeland security. The website provides original content through blogs and articles, which highlight federal programs, initiatives, webinars, and research. "Technology Profiles" display DHS-funded research and technologies by state. FirstResponder.gov also categorizes information by discipline: medical, explosives, fire, hazardous materials, law enforcement, and search and rescue. The website also provides a user feedback mechanism via email at: first.responder@dhs.gov. Visit www.firstresponder.gov.

First Responder Communities of Practice is an online network, sponsored by DHS Science and Technology First Responders Group, for vetted active and retired first responders, emergency response professionals; federal, state, local, tribal, and territorial Homeland Security and government officials, academic, non-profit, and volunteers sponsored by the DHS S&T's First Responder Technologies program. Registered members of this professional network share information, ideas, and best practices, enabling them to more efficiently and effectively prepare for all hazards. To date, First Responder Communities of Practice has more than 7,000 active members and nearly 200 active communities based on diverse interests and disciplines. For more information, visit www.firstresponder.gov or https://communities.firstresponder.gov.

The **First Responder Resource Group (FRRG)** serves as a mechanism for continuous dialogue and the coordination of research, development and delivery of technology solutions to first responders and the emergency preparedness and response community at the federal, state, local, tribal, and territorial levels. More than 120 responders from around the country are engaged throughout S&T's established solution development process to identify, validate, and facilitate the fulfillment of first responder needs through the use of existing and emerging technologies, knowledge products, and standards. The group meets annually in person and virtually throughout the year. To learn more about the FRRG, contact SandTFRG@dhs.gov.

International Consortium for First Responder Research and Development is being established by FRG to collaborate with international partners to consolidate common first responder capability gaps; share knowledge and networks with industry, academia, developers and innovators; and support the aggregation of the global first responder market. In order to respond more effectively, safely, and efficiently to everyday and catastrophic emergencies, first responders around the globe need technologically advanced tools and equipment. However, there is no centralized mechanism for them to identify and discuss shared needs and requirements. In addition, they tend to purchase tools and equipment in small quantities, which provides little incentive for industry to commercialize innovative technologies. The lack of consolidated requirements for first responders, along with the limited purchasing, results in an inadequate amount of new technology being available. This leads to an insufficient amount of research & development (R&D) being conducted in the first responder market. The goal of the International Consortium for First Responder R&D is to work collaboratively with international partners to improve first responder capabilities. To learn more about the International Consortium for First Responder R&D contact SandTFRG@dhs.gov.

The **National Urban Security Technology Laboratory (NUSTL)** is tasked with the mission to test, evaluate, and analyze Homeland Security capabilities while serving as a technical authority to first responder, state, and local entities in protecting our cities. In executing its mission, the Laboratory serves as a federal technical authority promoting the successful development and integration of homeland security technologies into operational end-user environments by objectively:

- Conducting test programs, pilots, demonstrations, and other forms of evaluations of homeland security technologies, both in the field and in the laboratory.
- Leveraging knowledge of end-user operations for

more effective development of technologies, training and exercises, ConOps, and procedures.

- Enabling first responders to meet their mission requirements by supporting them in the development of operational requirements and advising them on potential solutions to meet these needs.
- Supporting development and use of homeland security equipment and operational standards.

For more information, visit www.dhs.gov/science-and-technology/national-urban-security-technology-laboratory.

The **Office of Standards,** within the Capability Development Support Group facilitates the development and integration of standards across the entire spectrum from innovation to operations. The Office works closely with federal, state, and local law enforcement partners to identify, developB and promulgate standards through InterAgency Board's (IAB) Standardized Equipment List (SEL) and the FEMA Authorized Equipment List (AEL) for the law enforcement community's needs. In addition, the Office works with the National Institute of Justice (NIJ) and the National Institute of Standards and Technology (NIST) to promote the development and availability of relevant standards and associated conformity assessment programs for products and equipment listed in FEMA AEL. The Office has also entered into agreement with ASTM International to facilitate the procurement actions of the responder and law enforcement community by making standards available to state and local law enforcement and responder organizations at no cost. The Office is currently involved in developing standards for bomb squad robots, personal protective equipment, urban search and rescue robots, communications equipment, chemical and biological detectors among others that directly address needs expressed by the law enforcement community. For more information, contact Standards@hq.dhs.gov.

Project 25 Compliance Assessment Program (P25 CAP) was established, in coordination with NIST, to provide a process for ensuring that first responder communications equipment complies with P25 standards, meets performance requirements, and is capable of interoperating across manufacturers. P25 standards are focused on developing radios and other components that can interoperate regardless of manufacturer. P25 CAP allows emergency responders to confidently purchase and use P25-compliant products, and the Program represents a critical step toward allowing responders to communicate with their own equipment. In 2009, the first eight laboratories were officially recognized by DHS as part of the P25 CAP. A DHS-approved laboratory is authorized to produce summary and detail test reports for P25 equipment. For more information, visit www.llis.dhs.gov/knowledgebase/certifications-declarations.

The **Responder Technology Alliance (RTA)** was established by FRG to reframe the discussion among first responders, industry and investment community, and other research and development organizations to address current and future emerging technologies. The goal of the program is to leverage resources and expertise to deliver integrated responder solutions at "market speed." RTA is designed to bring a diverse set of stakeholders together to explore innovative technology solutions, standards formulation, and commercialization approaches to improve responder health, safety, and effectiveness. RTA focus areas are: (1) Body-Worn Electronic Systems; (2) Integrated Voice and Data Communications; (3) Multiple Hazard Personal Protective Clothing and Equipment (PPE); and (4) Advance Sensors and Information Technologies. RTA's goal is to work with industry to change the dynamic from first responder R&D efforts that are short-term and incremental with fragmented solutions often resulting in marginal, incremental improvements to operations and interoperability, to solutions that are innovative, well integrated and make the Nation's first responders safer. To learn more about RTA contact SandTFRG@dhs.gov.

System Assessment and Validation for Emergency Responders (SAVER) Program assists emergency responders making procurement decisions by providing subjective assessments of commercial responder equipment and systems. SAVER provides those assessment results along with other relevant responder equipment information in an operationally useful form. SAVER focuses primarily on answering two questions: "What equipment is available?" and "How does it perform?" The Knowledge Products produced by the SAVER Program are available to the responder community through www.firstresponder.gov/SAVER

Video Quality in Public Safety (VQiPS) Working Group was formed to focus on the major policy, technology, and practical uses and challenges of public safety video systems. The working group is comprised of emergency responders across all levels of government, academia, federal partners, and industry. The VQiPS Working Group creates knowledge products, fosters a knowledge-sharing environment, and supports research, development, testing, and evaluation for enhanced video quality through measurable, objective, and standards-based solutions across the full spectrum of video-use cases for the public safety community. For more information, contact VQiPS@hq.dhs.gov

Virtual Training provides a virtual environment that every jurisdiction within the country will be able to access, train within, and modify to meet their individual needs. S&T is leveraging investments and technological advances made by the military, specifically the U.S. Army's prototype virtual environment called Enhanced Dynamic Geo-Social Environment (EDGE) Virtual Training. S&T is using EDGE to develop a series of realistic, first responder-identified scenarios. The scenarios will have varying levels of difficulty and will require users to successfully employ tactics, techniques, and procedures to respond. The tool also has a strategic component requiring responders to establish Unified Command to manage complex cross discipline events. S&T worked with first responders to identify critical incidents and chose an active shooter for the first scenario and with the U.S. Army to create a 3-D environment for the scenario, as well as accurate avatars, equipment, and simulations of individuals and crowds. Following initial development, S&T conducted a pilot to demonstrate this scenario with emergency response agencies in Sacramento, California, and is currently upgrading EDGE with feedback collected from the Sacramento exercise. Eventually, S&T plans to incorporate this scenario, as well as others, into a customizable, multi-player online game that is interoperable with multiple user interfaces (e.g., joy stick, keyboard, gaming console). To learn more about simulation tools for first responders, contact SandTFRG@dhs.gov.

United States Secret Service (Secret Service)

The mission of the Secret Service is to safeguard the nation's financial infrastructure and payment systems to preserve the integrity of the economy, and to protect national leaders, visiting heads of state and government, designated sites and National Special Security Events.

Computer Emergency Response Team (CERT) at Carnegie Mellon. In August 2000, the Secret Service and the Software Engineering Institute, a federally-funded research and development center located at Carnegie Mellon University, instituted the Secret Service Computer Emergency Response (CERT) liaison program. This program positions the Secret Service to meet emerging cyber security threats as part of the agency's investigative and protective missions. The agents assigned to the CERT liaison program lead Secret Service-sponsored research and development as well as direct technical support for investigative and protective operations. The agents assigned to the CERT liaison program work closely with the Software Engineering Institute and Carnegie Mellon University to identify and implement advanced technology in support of the full spectrum of Secret Service operations. CERT does distribute forensic tools developed at the university to state and local law enforcement agencies. For more information, visit http://www.cert.org/digital-intelligence/index.cfm.

Cyber Intelligence Section (CIS) collects, analyzes, and disseminates data in support of Secret Service investigations worldwide and generates new investigative leads based upon this intelligence. CIS leverages digital equipment and information obtained through private partnerships to monitor developing technologies and trends in the financial payments industry. This information is used to enhance the Secret Service's capabilities to prevent and mitigate attacks against the financial and critical infrastructures. CIS has developed an operational investigative unit, which targets, pursues, and arrests international cyber criminals involved in cyber intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. CIS provides crucial information and coordination to facilitate the successful dismantling of international criminal organizations. Requests for investigative assistance should be facilitated through your local Secret Service Field Office at http://www.secretservice.gov/contact/field-offices/ or contact your local ECTF at http://www.secretservice.gov/investigation/#field.

eInformation Network. The Secret Service's eInformation Network is available – for free – to authorized law enforcement officers, financial institution investigators, academic partners, and commercial partners of the Secret Service. The site contains two tools: the eLibrary, a unique collection of resource databases which allows authorized users from throughout the law enforcement community to obtain information on a range of sensitive topics including counterfeit corporate checks, credit card issuing bank information, and recovered skimming devices; and the U.S. Dollars Counterfeit Note Search, a site that provides the user with the ability to conduct a search of the Secret Service counterfeit note database. For more information, visit www.einformation.usss.gov.

Electronic Crimes Special Agent Program (ECSAP). ECSAP trained specialists conduct forensic examinations of computers, mobile devices, and other electronic media. These agents possess the required expertise to collect and process digital evidence to support computer related investigations in the field. They also provide expertise in the investigations of network intrusions and database thefts. The program provides a venue that establishes and maintains relationships with the private sector in order to sustain and continually improve its knowledge of emerging trends in the cyber industry. ECSAP agents conduct forensic examinations for other federal, state, or local law enforcement upon request. For more information, please contact your local Secret Service Field Office at http://www.secretservice.gov/investigation/#field or contact your local ECTF at http://www.secretservice.gov/investigation/#field.

Electronic Crimes Task Force (ECTF). The USA PATRIOT Act of 2001 mandated the Secret Service to establish nationwide Electronic Crimes Task Forces to combine the resources of academia; the private sector; and local, state, and federal law enforcement agencies to *"prevent, detect and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."* There are currently 39 Secret Service ECTFs, to include London, England and Rome, Italy. Membership in the Secret Service ECTFs include approximately 350 academic partners; over 2,500 international, federal, state, and local law enforcement partners; and over 4,000 private sector partners. Through the ECTFs, local and state law enforcement officers may request investigative assistance from the Secret Service's Mobile Wireless Investigations teams. There are currently 22 MWI teams throughout the United States. For more information, visit http://www.secretservice.gov/investigation/#field. Also see ICE section above.

Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of Treasury, provides financial transaction information to law enforcement at the federal, state, local, and international level. FinCEN enhances the integrity of financial systems by facilitating the detection and deterrence of financial crime, by receiving and maintaining financial transactions data; analyzing and disseminating that data for law enforcement purposes; and building global cooperation with counterpart organizations in other countries and with international bodies. FinCEN utilizes numerous databases to provide intelligence and analytical support to law enforcement investigators protecting the U.S. financial system from the abuses of criminal activities to include terrorist financing, money laundering, and other illicit activity. For more information, please contact your local Secret Service Field Office at http://www.secretservice.gov/contact/field-offices/.

Financial Crimes Task Forces (FCTF). The Secret Service through years of collaboration on investigative endeavors established unique partnerships with state, local, and other Federal law enforcement agencies. Leveraging those partnerships with the agencies long-standing cooperation with the private sector, the Secret Service established a national network of Financial Crimes Task Forces (FCTFs). The FCTFs combine the resources of the private sector and other law enforcement agencies in an organized effort to combat threats to our financial payment systems and critical infrastructures. The multi-agency components are well suited to conduct complex, in-depth, multi-jurisdictional investigations. Through their membership in a FCTF, local and state law enforcement entities may access investigative resources to include FinCEN, INTERPOL, and IOC-2 databases. For more information, please contact your local Secret Service Field Office at http://www.secretservice.gov/contact/field-offices/.

International Organized Crime Intelligence and Operations Center (IOC-2). The U.S. Department of Justice's IOC-2 marshals the resources and information of nine U.S. law enforcement agencies, as well as federal prosecutors, to collectively combat the threats posed by international criminal organizations to domestic safety and security. The Secret Service IOC-2 detailee serves as the liaison between the Secret Service and the IOC-2 acting as a conduit for information and requests in support of field agents. For more information, please contact your local Secret Service Field Office at http://www.secretservice.gov/contact/field-offices/.

Mobile Device Forensic Facility. The Mobile Device Forensic Facility in Tulsa, OK was created in 2008 to meet the challenges associated with the forensic extraction of data from mobile devices. The Secret Service established a partnership with the University of Tulsa, Digital Forensic Laboratory Center of Information Security to create and co-locate the Mobile Device Forensic Facility at the University. The facility provides training and conducts forensic examinations and research on mobile devices. The ongoing research into these new devices, operating systems and mobile device technologies provides valuable tools in the Secret Service's fight against cybercrime. Requests for investigative assistance should be facilitated through your local Secret Service Field Office at http://www.secretservice.gov/contact/field-offices/.

National Center for Missing and Exploited Children. The Secret Service supports the National Center for Missing and Exploited Children and local law enforcement with its expertise in forensic analysis to include crime scene, handwriting, document authentication, ink analysis, fingerprints and photography, graphic design, video productions, audio/image enhancement and speaker recognition services. Specialized polygraph and crime scene services are evaluated upon request. For more information, visit http://www.missingkids.com/home and http://www.secretservice.gov/investigation/#forensic.

National Computer Forensics Institute (NCFI) – Hoover, AL. The NCFI was established in 2007 through a partnership initiative between DHS, the Secret Service, and the Alabama District Attorneys Association. The NCFI offers state and local law enforcement officers, prosecutors, and judges a variety of cyber-related training courses based on the Secret Service electronic crimes training model. NCFI offers the following 15 courses: Basic Investigation of Computer and Electronic Crimes Program, Basic Scripting Techniques, Basic Computer Evidence Recovery Training, Advanced Forensics Training, Basic Network Investigation Training, Network Intrusion Response Program, Basic Mac Investigation Training, Basic Mobile Device Investigations, Mobile Device Examiner, Advance Mobile Device Examiner, Online Social Networking, Computer Forensics in Court – Prosecutors, Computer Forensics in Court – Judges, Mobile Devices in Court – Prosecutors and Mac Forensics Training. NCFI provides funding for all travel expenses, hotel and per diem for state and local law enforcement officers. Additionally, all NCFI graduates receive hardware, software and licenses necessary to conduct forensic computer and network intrusion examinations. For more information, visit www.ncfi.usss.gov.

Transportation Security Administration (TSA)

TSA protects the nation's transportation systems to ensure freedom of movement for people and commerce.

Assistant Federal Security Directors for Law Enforcement (AFSDs-LE)
The AFSD-LE, working under the direction of the Federal Security Director (FSD), works to establish and maintain liaison with local, state, and federal law enforcement authorities, as well as coordinate activities taking place within their assigned transportation domain, on behalf of TSA's Office of Law Enforcement/Federal Air Marshal Service.

Typical liaison contacts for the AFSDs-LE may include airport police authority, Transportation Security Officers, Immigration and Customs Enforcement, the Joint Terrorism Task Force, Customs and Border Protection, the TSA Office of Inspection, and any other local, state, and/or federal agencies whose investigative interests may have a nexus to the transportation system within TSA's area of responsibility. For more information on TSA's AFSD-LE program, visit the TSA Website or contact your OLE/FAMS Supervisory Air Marshal in Charge (SAC) or FSD.

Commercial Vehicle Counter-Terrorism Training. Created under commission by TSA, the DHS Federal Law Enforcement Training Center (FLETC) worked directly with state, federal and municipal law enforcement agencies to identify the most effective ways for on-site officers to identify and intercept commercial vehicle-borne terrorist threats. Training at FLETC facilities or to law enforcement units at their home stations has been certified as eligible for DHS reimbursement through state assistance programs. Visit the FLETC website for more information: https://www.fletc.gov/training-program/commercial-vehicle-counterterrorism-training-program or contact the FLETC Glynco office at 912-267-3587.

Counter-Terrorist Guides. Pocket-sized publications directed to surface transportation providers in highway, mass transit, passenger and freight rail and pipeline modes identify terrorist techniques, motivation and opportunities to disrupt potential threats. These colorful guides have become many of the TSA Surface Division's most popular publications. For more information visit online at https://www.tsa.gov/stakeholders/resources-and-reports-1 or write to TSA-Surface@tsa.dhs.gov.

DVD Training – *Protecting Pipeline Infrastructure: The Law Enforcement Role*. Identifying a gap in the existing training materials, TSA developed this DVD training program to enhance the understanding of pipeline systems and their security issues by law enforcement officials. This DVD provides a basic understanding of how pipeline systems function, the principal products they transport, as well as a description of the threats to, and vulnerabilities of, pipelines. Law enforcement officials will achieve a better understanding of the usual measures taken to protect pipelines, and actions they can take to assist in this effort during times of heightened security. For more information and to order your training materials, visit www.tsa.gov/stakeholders/training-and-exercises.

First Observer Security™ Domain Awareness Training. Available online at TSA.gov, training modules speak directly to transportation professionals to enhance their understanding of terrorist techniques and threats, providing a message of "Observe, Assess, Report." Modules are currently available for highway-related professions. A new generation of messages similarly created will focus on those working in mass transit, passenger and freight rail and pipeline modes. More than 96,000 civilian transportation workers have been trained to date and TSA's domain awareness programs have been directly credited with disrupting two terrorist events. Learn more by writing to FirstObserver@tsa.dhs.gov or online at https://www.tsa.gov/first-observer.

Intermodal Security Training and Exercise Program (I-STEP) provides exercise, training, and security planning tools and services to the transportation community. I-STEP is the only federal exercise program to focus on the security nexus of the intermodal transportation environment. As a result, it not only reduces risk to individual systems, but the entire transportation network. Working in partnership with the various transportation modes, I-STEP provides a variety of products and services that enable security partners to enhance security capabilities by participating in and conducting exercises and training that strengthens security plans, test emergency procedures, and sharpen skills in incident management. I-STEP builds partnerships by collaborating with modal partners, law enforcement personnel, first responders, medical professionals, government leaders, and industry representatives to address challenges in transportation security. For more information, contact the I-STEP Program Office at 571-227-5150 or ISTEP@dhs.gov.

- Managed by the I-STEP, the **Exercise Information System (EXIS)** is the only exercise tool specifically tailored to the transportation sector. EXIS takes a step-by-step approach as it guides users though exercise planning. First it directs users to identify the exercise planning schedule and sector focus; next it enables users to select specific objectives and scenario elements; and finally, it allows users to plan evaluation criteria, share best practices and lessons-learned, and create post-exercise reports. EXIS communities facilitate information sharing among users. Users can create private communities and sub-communities to design operator-specific exercises and to delegate tasks to other planning team members. EXIS is provided at no cost by the TSA as an integral part of I-STEP. To become an EXIS member, visit http://exis.tsa.dhs.gov. For more information, contact EXIS@dhs.gov.

Joint Vulnerability Assessment (JVA) Training. The Security Assessments Section (SAS), under the Office of Law Enforcement/Federal Air Marshal Service, Security Services and Assessments Division conducts JVAs in partnership with the FBI for the purpose of assessing current and potential threats to commercial air transportation facilities within the United Sates. The assessment process is a direct result of the increasing threat to aviation, a threat which prompted Congress to pass Section 310 of the Federal Aviation Reauthorization Act of 1996, requiring the Federal Aviation Administration (FAA) and the FBI to conduct joint threat and vulnerability assessments of security at U.S. airports. In response to this mandate, during Fiscal Years (FY) 1999, 2000, and 2001, FAA and FBI prepared three-part assessments addressing the vulnerability, criminal activity, and terrorist threat at selected airports nationwide. In Fiscal Year 2002, TSA took on the responsibility of conducting assessments from the FAA pursuant to the Aviation and Transportation Security Act. SAS conducts JVAs in order to identify vulnerabilities and recommends options to mitigate those vulnerabilities. SAS conducts JVA training as needed and it can be made available to local law enforcement and security personnel upon request. For more information, contact OLEFAMSSAS@dhs.gov.

Law Enforcement Officer (LEO) Reimbursement Program provides partial reimbursement to state, local, or other public institutions or organizations responsible for commercial airport operations within their jurisdiction, as specified in U.S. statute or TSA program guidance documents and regulations. Funding is intended to help defray the cost of providing highly visible law enforcement presence and support of passenger screening activities at U.S. commercial airports. For more information, visit www.tsa.gov/about-tsa/law-enforcement-officer-leo-reimbursement.

Man-Portable Air Defense Systems (MANPADS) Awareness Training. MANPADS are portable surface to air guided missile systems designed to be carried by an individual. The SAS, under the Office of Law Enforcement/Federal Air Marshal Service, Security Services and Assessments Division, conducts MANPADS Vulnerability Assessments (MVA) at commercial airports nationwide in an effort to identify and define potential launch areas, areas that are rated on the basis of seven specific characteristics. A multi-dimensional approach is designed to detect, deter, and defeat a MANPADS threat against civil aviation. SAS also provides oversight and guidance on the development and implementation of MANPADS mitigation plans at the commercial airports.

SAS provides a MVA Basic Training Program (MVABTP) course that provides field personnel with the basics on how to conduct a MVA and the requirements for the MMP. In addition, it will provide knowledge on how to identify areas of concern for other stand-off weapons threats. Report templates, reference and briefing material will be provided to all trainees.

SAS provides MANPADS awareness training and outreach to local law enforcement and other first responders. The Law Enforcement MANPADS Awareness Training Program (LEMATP) provides law enforcement and other first responders with the basic knowledge on how to mitigate an attack. The course includes MANPADS capabilities, SAS MVA methodology and selection of sites, the requirements for a MMP, patrol/security techniques, law enforcement response to a MANPADS attack, and investigative tips after a

MANPADS attack. TSA also provides MANPADS pocket identification cards and posters to law enforcement and first responders to assist in the identification of MANPADS and their components.
For more information, contact OLEFAMSSAS@dhs.gov.

Canine Training Center (CTC). The Office of Training and Workforce Engagement CTC supports the TSA mission by providing highly trained Explosives Detection Canine teams for deployment throughout the Nation's transportation systems. The canine teams provide explosive detection capabilities, visible deterrence, and a timely and mobile response to security incidents. These highly trained canine teams are trained to work within the major transportation environments, i.e., aviation, maritime, mass transit surface, and rail, to detect various explosives odors. Detection capabilities include, but are not limited to, the following: aircraft, trains, ferries, cruise ships, vehicles, passenger terminals, cargo, baggage, as well as people and items either concealed on their person or in their possession. The capabilities provided by these canine teams offer a very proficient layer of security in our Nation's transportation systems in support of the TSA mission.

Sensitive Security Information (SSI) Program. Sensitive Security Information (SSI) is information obtained or developed which, if released publicly, would be detrimental to transportation security, and is defined at 49 CFR Part 1520. SSI is not authorized for public disclosure and is subject to handling and safeguarding restrictions.

The TSA SSI Program, the central SSI authority for all of DHS, develops SSI guidance and training materials to assist state and local law enforcement partners in the recognition and safeguarding of SSI. The SSI Program also develops SSI policies and procedures, analyzes and reviews records for SSI content, and coordinates with stakeholders, other government agencies and Congress on SSI-related issues.

For more information about SSI or for assistance in identifying SSI, visit https://www.tsa.gov/for-industry/sensitive-security-information or contact 571-227-3513 or SSI@dhs.gov.

The **TSA Call Center (TCC)** is responsible for fielding incident reports from the public. TSA's Internal Affairs Division (IAD) is responsible for conducting criminal and administrative investigations of employees who are alleged to have committed misconduct, including identifying and investigating potential worker's compensation fraud by TSA employees. If a person suspects that a TSA employee is engaging in misconduct or fraud, they are asked to contact TSAInspectionHotline@tsa.dhs.gov and provide the name of the employee suspected for alleged misconduct and an explanation of the issue, including date(s) and time(s). They are also asked to provide their name and contact information for appropriate follow-up. Employees should provide their name even if they choose to remain anonymous throughout the process. The public may also report security-related incidents to TCC, and may request follow up information on the status of those reports through TCC.

TSA Law Enforcement Officer (LEO) Flying Armed Training Program. The TSA Office of Training and Workforce Engagement, Law Enforcement and Industry Training Division is responsible for oversight of the TSA LEO Flying Armed Training Program, which is *mandatory* for all law enforcement officers flying armed under the Code of Federal Regulation 1544.219, Carriage of Accessible Weapons. The LEO Flying Armed training is a 1.5 to 2 hour block of instruction that is comprised of a structured lesson plan, slide presentation, FAQs, NLETS procedures, and applicable codes of Federal regulation. This material is provided to federal, state, local, territorial, tribal, and approved

railroad law enforcement agencies and departments to properly instruct their officers on the subject of flying on board commercial aircraft while armed. The training includes protocols in the handling of prohibited items, prisoner transport, and dealing with an act of criminal violence aboard an aircraft. The program training material may be obtained by emailing the TSA Office of Training and Workforce Engagement, Law Enforcement and Industry Training Division, at LEOFA@dhs.gov
To request this training material you must:

- Be a full-time law enforcement officer meeting the instructor qualification standards of the agency, academy, or department in which you are employed;
- Send the request from a governmental email address; and
- Include the following information in the body of the email: (1) Your name and contact information; (2) Your department's name and address; and (3) Your supervisor's name and contact information.

If you are not a qualified instructor, please request a member of your training staff to contact us by email. For time sensitive training requests, please call (855) 359-5367 between the core business hours of 9:00 am to 5:00 pm EST.

Visible Intermodal Prevention and Response (VIPR) Program. Focusing on deterrence and detection of terrorist activities, TSA conducts VIPR operations that promote confidence in and protect all modes of transportation through targeted deployment of integrated TSA assets, coming from TSA's Offices of Law Enforcement and Security Operations.

The VIPR Program has a nationwide footprint. Applying a risk-based planning process, TSA conducts VIPR operations with state and local personnel on a random, unpredictable basis. VIPR operations are conducted in all modes of aviation and surface transportation. Teams may also be deployed to provide additional law enforcement or security presence at transportation venues during specific alert periods or in support of special events.

The exact makeup of a VIPR operation team is determined jointly with local authorities. An operation can include Federal Air Marshals, Transportation Security Officers, Behavior Detection Officers, Transportation Security Inspectors, and Transportation Security Specialists – Explosives, TSA personnel can use explosives operational support, security and explosive screening technology, and radiological/nuclear detection equipment.

For more information on TSA's VIPR resources, visit the TSA website or contact your OLE/FAMS Supervisory Air Marshal in Charge (SAC) or Federal Security Director (FSD).

ACRONYMS

ACAMS	Automated Critical Asset Management System
AEL	Authorized Equipment List
AMOC	Air and Marine Operations Center
ANSI	American National Standard Institute
BCOT	Building Communities of Trust
BCSC	National Bulk Cash Smuggling Center
BEST	Border Enforcement Security Task Force
BMAP	Bomb-making Material Awareness Program
BPA	Blanket Purchase Agreement
BSC	Biometric Support Center
C3	Cyber Crime Center
CAB	Community Awareness Briefing
CAP	Criminal Alien Program
CBP	U.S. Customs and Border Protection
CBRNE	Chemical, Biological, Radiological, Nuclear and Enhanced Conventional Weapons
CCU	Cyber Crimes Unit
CDF	Capability Development Framework
CDM	Continuous Diagnostics and Mitigation
CDP	Center for Domestic Preparedness
CEIU	Child Exploitation Investigation Unit
CERT	Computer Emergency Response Team
CFATS	Chemical Facility Anti-Terrorism Standards
CFU	Computer Forensics Unit
CGMIX	USCG Maritime Information eXchange
CI	Critical Infrastructure
CIFW	Counterintelligence Fundamental Workshop
CIPD	Counterintelligence Division
CIS	Cyber Intelligence Section
CMaaS	Continuous Monitoring as a Service
COE	Centers of Excellence
COI	Community(ies) of Interest
COML	Communications Unit Leader
COMT	Communications Unit Technician
COP	Common Operating Picture
CP	Continued Presence
CPAA	Cultural Property, Art, and Antiquities
CRCL	Office for Civil Rights and Civil Liberties
CRR	Cyber Resiliency Review
CSEP	Cybersecurity Evaluation Program
CVE	Countering Violent Extremism
CVEC	Countering Violent Extremism Coordinator
DARTTS	Data Analysis & Research for Trade Transparency Systems
DBFTF	Document and Benefit Fraud Task Force
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DHS-SPS	DHS Single Point of Service
DMV	Department of Motor Vehicles
DNDO	Domestic Nuclear Detention Office
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DSF	Deployable Special Forces
ECSAP	Electronic Crimes Special Agent Program
ECTF	Electronic Crimes Task Force
EDCT	Explosive Detection Canine Team
EDD	Explosive Detector Dog
EDGE	Enhanced Dynamic Geo-Social Environment
EMI	Emergency Management Institute
EOC	Emergency Operations Center
ERO	ICE Enforcement and Removal Operations
ESS	Emergency Sector Services
ESS-CRA	Emergency Sector Services-Cyber Risk Assessment
EXIS	Exercise Information System
FAA	Federal Aviation Administration
FAR	Fugitive Alien Removal
FBI	Federal Bureau of Investigation
FCTF	Financial Crimes Task Force
FDNS	Fraud Detection and National Security
FEDSIM	Federal Systems Integration and Management Center
FEMA	Federal Emergency Management Agency
FinCEN	Financial Crimes Enforcement Network
FiRST	First Responder Support Tool
FLETC	Federal Law Enforcement Training Centers
FOT	Fugitive Operations Teams
FOUO	For Official Use Only
FPS	Federal Protective Services
FRG	First Responders Group
FRRG	First Responder Resource Group
FSCC	Federal Sponsored Course Catalog
FSLTT	Federal, State, Local, Tribal, Territorial
FY	Fiscal Year
GNDA	Global Nuclear Detection Architecture
GPD	Grant Programs Directorate
GPS	Global Position System
GSA	General Services Administration
HAZMAT	Hazardous Materials
HME	Homemade Explosives
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSDN	Homeland Security Data Network
HSI	ICE Homeland Security Investigations
HSIN	Homeland Security Information Network
I&A	Office of Intelligence and Analysis
IAB	Interagency Board
IAD	Internal Affairs Division
IAQ	Immigration Alien Query
IC	Intelligence Community
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronics Engineers
ICE	U.S. Immigration and Customs Enforcement

ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICTAP	OEC Interoperable Communications Technical Assistance Program
IDENT	Automated Biometric Identification System
IMAGE	ICE Mutual Agreement between Government and Employers
IMPACT	Incident Management Preparedness and Coordination Toolkit
INTERPOL	International Criminal Police Organization
IOC-2	International Organized Crime Intelligence and Operations Center
IP	Intellectual Property
IPAWS	Integrated Public Alert and Warning System
IPR	Intellectual Property Rights
IPR Center	National Intellectual Property Rights Coordination Center
I-STEP	Intermodal Security Training and Exercise Program
ISIL	Islamic State of Iraq and the Levant
ITA	Intelligence Training Academy
JAC	Joint Analysis Center
JACCIS	JAC Collaborative Information System
JACTAWS	Joint Counterterrorism Awareness Workshop Series
JVA	Joint Vulnerability Assessment
LEO	Law Enforcement Officer
LESC	ICE Law Enforcement Support Center
LEISI	Law Enforcement Information Sharing Initiative
LEIS Service	Law Enforcement Information Sharing Service
LEMATP	Law Enforcement MANPADS Awareness Training Program
LES	Law Enforcement Sensitive
LESC	Law Enforcement Support Center
LMR	Land Mobile Radio
LMS	Learning Management System
MANPADS	Man-Portable Air Defense Systems
MCV	Mobile Command Vehicle
MDDP	Mobile Detection Deployment Program
MDDU	Mobile Detection Deployment Unit
MISLE	Marine Information for Safety and Law Enforcement
MJIEDSP	Multi-Jurisdictional Improvised Explosive Device Security Planning
MS-ISAC	Multi-State Information Sharing Center
MVA	MANPADS Vulnerability Assessments
MVABTP	MANPADS Vulnerability Assessments Basic Training Program
NBIC	National Biosurveillance Integration Center
NCAS	National Cyber Awareness System
NCATS	National Cybersecurity Assessment and Technical Services Teams
NCC	National Coordination Center
NCCAD	National Counter-IED Capabilities Analysis Database
NCCIC	National Cybersecurity and Communications Integration Center
NCEPP	National Cyber Exercise and Planning Program
NCFI	National Computer Forensics Institute
NCSAM	National Cybersecurity Awareness Month
NCTC	National Counterterrorism Center
NECP	National Emergency Communications Plan
NEDCTP	National Explosives Detection Canine Team Program
NFOP	National Fugitive Operations Program
NGI	Next Generation Identification
NGO	Nongovernmental Organization
NICC	National Infrastructure Coordination Center
NIMS	National Incident Management System
NIMS ICS	NIMS Incident Command System
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPPD	National Protection and Program Directorate
NPSBN	Nationwide Public Safety Broadband Network
NSI	Nationwide Suspicious Activity Reporting (SAR) Initiative
NTAS	National Terrorism Advisory System
NTED	National Training and Education Division
NUSTL	National Urban Security Technology Laboratory
OBIM	Office of Biometric Identity Management
OBP	Office of Bombing Prevention
OCIA	Office of Cyber and Infrastructure Analysis
OCP	Office of Community Partnerships
OCSTF	Operation Community Shield Task Forces
ODLS	Online Detainee Locator System
OEC	Office of Emergency Communications
OHA	Office of Health Affairs
OIG	Office of Inspector General
OSLLE	Office for State and Local Law Enforcement
OSLTC	ICE Office of State, Local, and Tribal Coordination
P25 CAP	Project 25 Compliance Assessment Program
PED	UCSIS Public Engagement Division
PEP	Priority Enforcement Program
PERC	Pacific Enforcement Response Center
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PLEPU	Parole and Law Enforcement Programs Unit
PM	Program Management
PPE	Personal Protective Equipment
PRIV	DHS Office of Privacy
PRND	Preventative Radiological/Nuclear Detection
PRD	Personal Radiation Detector
PSA	Protective Security Advisors
R&D	Research and Development
RAAS	Report Analysis and Archive System
RD	Regional Directors
RFI	Request for Information
RKB	Response Knowledge Base

RIID	Radiation Isotope Identification Device
RISS	Regional Information Sharing System
R/N	Radiological and Nuclear
RTA	Responder Technology Alliance
S&T	Science and Technology Directorate
SAS	Security Assessment Section
SBU	Sensitive but Unclassified
SCIP	Statewide Communication Interoperability Plan
SEL	Standard Equipment List
SEVP	Student Exchange Visitor Program
SLT	CBP State, Local, Tribal, Liaison
SLTD	State, Local, and Tribal Division
SLTT	State, local, tribal, and territorial
SPBP	Significant Public Benefit Parole
SSI	Sensitive Security Information
STC	Security the Cities
SWBCWG	Southwest Border Communications Working Grp.
SWIC	Statewide Interoperability Coordinator
TA	Technical Assistance
TBML	Trade-Based Money Laundering
TCC	TSA Call Center
TCO	Transnational Criminal Organization
TRIP*wire*	Technical Resource for Incident Prevention
TSA	Transportation Security Administration
TTU	Trade Transparency Unit
UASI	Urban Area Security Initiative
US-CERT	U.S. Computer Emergency Readiness Team
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USSS	United States Secret Service
VAP	Victims Assistance Program
VAWA	Violence Against Women Act
VBIED	Vehicle-borne Improvised Explosive Device
VIG	Vehicle Inspection Guide
VQiPS	Video Quality in Public Safety
VWP	Visa Waiver Program
WMD	Weapons of Mass Destruction

APPENDIX

From: Bogosian, Vicky
To: CTAB-All
Cc: CT Staff
Subject: 07.23.15 CTAB Agenda and Kenya CVE Summit Readout
Date: Wednesday, July 22, 2015 6:22:39 PM
Attachments: Kenya CVE Summit Readout.pdf

Good evening,

Please check your C-Lan account for this week's CTAB Agenda. In addition, Ms. Megan Mack committed to provide the Kenya CVE Summit readout last week at the CTAB meeting; please find her document attached in this email.

Reminder, the meeting is at 2:00 – 3:00 PM; Deputy Secretary Mayorkas is chairing and Principal Deputy CT Coordinator Gene Gray if facilitating. The location remains – NAC, Bldg. 19, Room 01-117.

Thank you,

R/Vicky

Vicky Bogosian,
CTAB Secretary, DHS HQ
(b) (6)

(U) Warning: This document contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policies and is not to be released to the public, the media, or other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official.

Office for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

July 21, 2015

MEMORANDUM FOR: Megan H. Mack
Officer for Civil Rights and Civil Liberties

Tamara Kessler
Deputy Officer for Civil Rights and Civil Liberties

THROUGH: (b) (6)
Section Lead, Community Engagement Section

FROM: (b) (6)
Senior Policy Advisor, Community Engagement Section

SUBJECT: Kenya CVE Regional Summit in Nairobi, Kenya, June 25-28, 2015

Purpose

This memorandum serves as a trip report for CRCL's participation in the Kenya CVE Regional Summit on June 25 -28, 2015, in Nairobi, Kenya.

Background

The Kenya CVE Regional Summit was organized by the Government of Kenya (GOK) in Nairobi, Kenya, to bring together CVE subject matter experts, practitioners, religious leaders, civil society leaders, non-governmental organizations (NGOs), government officials from around Africa, international governmental organizations (e.g., United Nations, European Union, African Union, and IGAD), and donor countries, including the United States, United Kingdom, France, Netherlands, Turkey, Indonesia, and Denmark. The Summit, a follow-up to the White House CVE Summit held in Washington, D.C. earlier this year, was designed to shed light on the challenges posed by violent extremist groups in East Africa and help regional authorities devise national CVE strategies. The U.S. Embassy in Kenya and the U.S. State Department provided significant financial and technical support. A 12-member delegation from the United States included [redacted] (b) (6), CRCL Senior Policy Advisor, and Ron Clark, NPPD Deputy Undersecretary. The

U.S. delegation was led by Sarah Sewall, Department of State Undersecretary, who represented the United States at the summit.

Remarks by Delegates and Host Government Officials

Welcoming remarks were provided by GOK Principal Secretary of the Ministry of the Interior, Monica Juma, who referenced the White House CVE Summit as the impetus for the GOK pledging to host a regional summit in East Africa. Principal Secretary Juma framed the GOK's assessment of the threat of terrorism in East Africa and concluded with an evaluation of the socioeconomic and geopolitical factors to consider in the development of GOK's national strategy on CVE.

Following the Principal Secretary's remarks, Undersecretary Sewall provided opening remarks on a wide range of challenges the global community faces, and among other things, underscored the vital role that civil society organizations play in the holistic approach necessary in the development and implementation of any meaningful national CVE strategy. Undersecretary Sewall expressed disappointment on behalf of the USG for the GOK's failure to include more civil society actors in the Summit and specifically mentioned the absence of MUHURI (Muslims for Human Rights) and Haki Africa (a Mombasa based Human Rights NGO) as a missed opportunity to add diverse civil society organizations into the problem-solving equation. Undersecretary Sewall highlighted initiatives to maintain the momentum on CVE activities among the various subsets of the international community, namely the development and launching of regional and global enterprises: the Strong Cities Network, youth, civil society, and research networks.

The opening session ended with remarks from William Rutto, Deputy President of Kenya, who stated that violent extremism is the "most pressing threat facing Kenya today." The Summit was closed by the President of the GOK, H.E. Kenyatta.

At the ministerial level meeting held on the last day of the Summit, the international community pledged support for CVE efforts in East Africa. Participants included: UN, EU, UK, USA, France, Egypt, Somalia, Eritrea, Netherlands, Turkey, Indonesia, Libya, Denmark, and Djibouti.

Key Findings

(b) (5) [redacted]

(b) (5) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Notable Sessions

Session on "Understanding the Architecture and Dynamics of Radicalization and Recruitment." Moderator: Principal Secretary Juma; Panelists: Dr. Karima Bennoune, Professor of Law at the University of California Davis, and Ambassador Samuel Assefa of Ethiopia. Dr. Bennoune's book, "Your Fatwa Does Not Apply Here," contains nearly 300 interviews of CVE workers and depicts their experiences standing up to terrorism. Speaking as the daughter of a prominent Algerian intellectual who viewed that "radical Islam" was brought by outside influencers demonstrating a radical break with Islam, Dr. Bennoune provided three key lessons learned:

1. Practical solidarity is critical in the aftermath of attacks and when facing increasing radicalization and recruitment;
2. "Jihadist" ideology is the perpetrator of the greatest amount of violence and murder across the world. There is a need to combat this source of violence at the same time as suppressing prejudice and discrimination against Muslims writ large; and
3. The importance of protecting human rights in the fight against terrorism. Nothing undermines governments more than suppression of human rights in the name of efforts to preserve security.

Dr. Bennoune stressed that Muslims are the majority of the victims of terrorist organizations and women's empowerment is necessary to CVE efforts. Her discussion describing terrorist organizations heavily relied on terminology that was rejected by many participants, including "jihadist," "islamic violence," "islamist," "islamic fundamentalist," and "fundamentalism." One participant from Kenya referenced and applauded the USG's careful use of non-inflammatory terminology to ensure that mainstream Muslim communities are not alienated and not lumped together with terrorist organizations.

Ambassador Assefa discussed how local context matters in violent extremist recruitment and stressed that global narratives can inspire (but not replace) local context such as lack of services, of democracy, and of rights, or the existence of poverty, corruption, marginalization, repression of minority rights, etc. He divided terrorist groups messaging into two models:

1. Model One: Reactionary, appeals to the converted and the local messaging; and
2. Model Two: Terrorists as marginalized from society. Motivations are not reactive, but loathing of "modernity" and the vulnerable individual who does not want to be part of an order that is void of spiritual values. This mostly is rooted in a deep seated grievance narrative and rejection of "the West," which oftentimes translates into rejection of democratic values and institutions, progress, enlightenment, and universalist values. Examples cited included Israel bombing Gaza, and the U.S. wars in Iraq and Afghanistan.

Ambassador Assefa concluded that violent extremist messages succeed because governments use the concept of protection of national security to destroy what is deemed to be the most valuable democratic values and freedoms. To succeed in national security efforts, civil liberties should be upheld.

Session on the "Local Architecture and Dynamics of Radicalization and Recruitment." Moderator: Ambassador Dr. Martin Kimani, Kenya's Ambassador to United Nations Office at Nairobi (UNON), United Nations Environment Program (UNEP), and United Nations Habitat. Ambassador Kimani discussed pathways to radicalization to violence stating that the pathway is highly individualized; however, the local architecture primarily comes from the family. Breakdown of family values likely leads to radicalization to violence. The Ambassador's discussion was grouped into three points:

1. Local recruitment networks use the following process: a) Identify vulnerable people (economic conditions, grievances, injustices); b) Identify individual incentives (money, religious purposes); c) Utilize transnational linkages (Boko Haram and Al-Shabaab).

2. Motivation for the individual comes in three forms: a) To express solidarity with the global Islamic causes; b) Jobs (mean age in Africa is 19 and they need hope); c) Romanticizing of violent extremist groups.
3. What is necessary for meaningful CVE in Africa: a) Good institutions and community involvement; b) Identifying those susceptible to radicalization to violence; and c) An end to conflicts in African countries—the majority of the most unstable countries are in Africa; 4) Mobilization of local populations.

Noteworthy, Ambassador Kimani mentioned positively the DHS community engagement program and the three-city pilot program, which he referred to as the DHS "strong cities program."

Rohan Gunaratna, Singapore (Professor at the Rajaratnam School of International Studies). Mr. Gunaratna shared his experience living in Africa and recognized that problems of radicalization to violence in Africa started in the 1980s; he asserted that Africa is an international epicenter for terrorism.

He proposed three steps to counter radicalization to violence:

1. Use of community engagement that parallels military and law enforcement operations;
2. Rehabilitation programs, particularly those in detention centers; and
3. Building coalitions to dismantle violent extremist organizations.

He also suggested that rehabilitation programs should have seven modes: 1) Spiritual and/or religious; 2) Education; 3) Vocation and skills; 4) Social and family; 5) Arts, sports, and recreation; 6) Social and mental health; and 7) Financial support.

(b)(6)

From: Bogosian, Vicky
Sent: Thursday, October 29, 2015 1:29 PM
To: CTAB-All; CTAB CYBER
Cc: Selim, George; Gersten, David; Snyder, Nathaniel; Taylor, Francis X; Gray, Eugene; Warrick, Thomas; CT Staff
Subject: 10.29.15 CTAB - OCP-CVE Action Plan Delivery
Attachments: DHS CVE Action Plan_clean 10 27 2015 (CLEAN).docx

Good morning,

As discussed at the CTAB this morning, we have attached a copy of the Office of Community Partnership (OCP-CVE) Action Plan for your files.

If you have questions or comments please contact either: OCP Director George Selim, or Deputy Director David Gersten and if they are not available reach out to Nathanial Snyder.

Please feel free to contact me if I can assist further.

Thank you,

R/Vicky

Vicky Bogosian,
CTAB Secretary, DHS HQ
(b) (6)

(U) Warning: This document contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policies and is not to be released to the public, the media, or other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official.

U.S. Department of Homeland Security Action Plan to Counter Violent Extremism

October 20, 2015

DHS Lines of Effort and Key Actions to Counter Violent Extremism

1. Encourage and enable our partners to counter violent extremism.

The family, friends, and acquaintances of a potential violent extremist are often best positioned to recognize a shift toward radicalization to violence and intervene early, while local service providers and community organizations are often best equipped to provide the personalized support an individual may need to choose a path that does not lead to violent extremism. DHS supports these community-based efforts to counter violent extremism (CVE) by raising awareness of the violent extremist threat, convening and connecting our partners to facilitate joint action against threats, and by providing tools and financial assistance.

Foundational Activities

DHS Office for Civil Rights and Civil Liberties (CRCL), in partnership with the National Counterterrorism Center (NCTC), provides **Community Awareness Briefings (CABs)** to diverse communities in cities across the country, where we share unclassified information regarding the threat that violent extremism poses to them and ways to address these threats. These briefings are designed to help communities and law enforcement develop the necessary understanding of terrorism and terrorist recruitment tactics and explore ways to collectively and holistically address these threats before they become a challenge at the local level.

Also in partnership with NCTC, DHS CRCL facilitates **Community Resilience Exercises (CREXs)**, half-day, table-top exercises designed to improve communication between law enforcement and the communities they serve.

DHS also conducts **training for law enforcement that includes CVE-focused curriculum.** Since 2010, DHS has trained nearly 18,000 students on all types of U.S.-based terrorism.

Further, the Department supports state, local, tribal, and territorial government partners as well as major urban area intelligence fusion centers by **sharing information** with state and local officials on threats.

DHS will continue to collaborate with federal interagency partners to support locally-developed and locally-driven prevention and intervention programs, including the **First Tier Three Cities Program**. Under this interagency program, public safety officials, religious officials, social workers, educators, community representatives, and U.S. Attorneys' Offices have developed their own regionally-tailored strategies to counter violent extremism in the First-Tier Three Cities - Boston, Los Angeles and Minneapolis.

Building on these foundational activities, DHS will augment and expand its efforts to support communities.

New Initiatives to Counter Violent Extremism

Technology companies and experts are uniquely positioned to assist community-based efforts to counter violent extremism. Social media, marketing, and technology industry partners can support community-based initiatives by helping parents keep their kids safe online, and offering their services and capabilities to community partners to promote effective CVE messages. These same companies and leaders have powerful platforms from which to shape public debate and discussion by introducing their own messaging and content and shaping the way that content appears on their applications, websites, and search results. **DHS will develop a digital implementation plan** to promote and support technology sector partners in using these unique capabilities to assist CVE efforts.

Community-based programs look to external support—whether from government or the private sector—to help them fund their efforts to counter violent extremism. DHS will support community-based CVE programs by **linking community programs with potential partners in the private sector**, to include philanthropies and foundations, and by **providing grant-based support** directly to community programs. DHS will continue to enhance our grant-making mechanisms to make grants more accessible for community-based organizations pursuing CVE programs.

To help our federal, state, local, tribal, and territorial government partners, including law enforcement, and community groups, become more informed about the threat of violent extremism and effective tools to counter it, DHS will **develop and share strategic threat assessments** with our partners. DHS will also **support the development of tools** to help community-based CVE program leaders assess the impact of their efforts.

Through the First-Tier Three Cities Program and DHS's Los Angeles-based Office for Strategic Engagement, DOJ, DHS and community leaders work together to build trust, identify capability and resource gaps, and facilitate capacity-building opportunities. Building on the success of these efforts, **DHS will expand its full-time presence in first-tier cities** (Boston, Los Angeles, and Minneapolis).

Across DHS CVE programming, the Department will place greater emphasis on **measuring program impacts and effectiveness.**

DHS Actions to Counter Violent Extremism

1. Encourage and enable our partners to counter violent extremism.

Activity and Milestones	Lead Office	Target Date
FOUNDATIONAL ACTIVITIES		
Enhance community understanding of the threat and effective measures to counter violent extremism. - Help communities develop an understanding of	CRCL	Community Roundtables, Briefings,

recruitment tactics and explore ways to collectively address threats at the local level by continuing to improve and expand Community Engagement Roundtables, Community Awareness Briefings (CAB), and Community Resilience Exercises (CREX) to cities across the country. - By November 1st, provide a plan including the following: - A calendar of proposed community roundtables, briefings and exercises in specific communities. - For each roundtable, briefing and exercise, identify: regionally-specific goals and objectives; community-based programs we want to highlight; organizations and institutions who could be helpful partners; recommended senior leader participants; and recommended post-engagement actions. - Strategic objectives: specify what we hope to accomplish through the roundtables, briefings and exercises, and how to capture what we have learned from these efforts. - Provide quarterly updates detailing progress, lessons learned, and upcoming milestones or targets.		Exercises: ongoing. Plan is due by November 1, 2015. First quarterly update due January 2016.
Enhance training for federal, state, local, tribal, and territorial law enforcement. - Provide federal, state, local, tribal, and territorial law enforcement with the tools and training they need to recognize and effectively respond to potential instances of radicalization to violence. - Update CVE-relevant components of training programs (including the Uniformed Police Training Program, Criminal Investigator Training Program, Land Management Police Training Program, and the Rural Police Officer Training) in consultation with FLETC's impacted federal partner organizations to ensure that such training components reflect current assessments of the violent extremist threat. - Provide train-the-trainer programs, cultural competency, and violent extremism awareness training to additional state, local, tribal, and territorial law enforcement partners. - Provide three hours of CVE-specific training during the Homeland Security Leadership Academy, an eight-day training program for state and local law enforcement executives.	**FLETC** **FEMA** **CRCL** **OCP**	Law enforcement training: ongoing. Plan to update and expand training is due by November 1, 2015. First quarterly update due January 2016.

- By November 1st, provide a plan to accomplish these three tasks. The plan should include specific milestones and targets. - Provide quarterly updates detailing progress in reaching milestones, and lessons learned.		
Develop and share intelligence assessments with state, local, tribal, territorial, and community partners. - Provide timely information on current threat streams and trends related to violent extremism recruitment, tactics, and targets. - Expand the distribution of DHS Intelligence and Analysis-originated terrorism reporting to ensure this reporting is accessible to vetted homeland security stakeholders. - Disseminate classified and unclassified assessments and briefings on threats and trends related to violent extremism to DHS Components, fusion centers, police departments, and other federal, state, and local law enforcement partners. These assessments and briefings should include topics such as recruiting methods and narratives used by domestic terrorist and foreign terrorist organizations and Western foreign fighters. - Maintain and update the joint DHS/FBI Countering Violent Extremism and Active Shooter Web Portal on the Homeland Security Information Network. - Provide quarterly updates detailing progress, lessons learned, and upcoming milestones or targets.	**I&A**	Information sharing and web portal maintenance: ongoing. First quarterly update due January 2016.
Evaluate DHS progress in meeting targets in the 2011 White House Strategic Implementation Plan. - Provide a report on DHS progress in meeting requirements set forth in the 2011 White House Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States.	**OCP**	Report is due by October 9, 2015.

Awareness level on line training for state, local, tribal and territorial law enforcement line officers, supervisors, and training academy directors. - Raise awareness and understanding of violent extremism for state, local, tribal and territorial law enforcement partners. - Identify the differences between Constitutionally-protected cultural, societal, and religious behavior versus indicators of criminal behavior. - Definition and examples of radicalization. - How to assess threats and potential targets. - The implications on officer safety. - The importance of building partnerships with community organizations. - Understanding different cultures and people. - The importance of community policing. - How to engage community members in preventing acts of terrorism and violent extremism. - Provide quarterly updates detailing progress, lessons learned, and upcoming milestones or targets.	**FEMA NPD**	Curriculum Review - November 2015. Anticipated availability - February 2016. Target audience: Law enforcement line officers, supervisors, and training academy directors.
Awareness level online training for state, local, tribal and territorial Community Liaison Officers, School Resource Officers, NGOs and community leaders. **The two online courses in development are Radicalization Awareness for Community Engagement and Resilience, and Community Resilience to Violent Extremism.** - Provide community-focused, rigorously-researched and academically-informed instruction on countering violent extremism. - Define the mechanisms by which individuals and groups develop a willingness to use violence to advance an ideological cause. - Describe how communities can engage in efforts that will make individuals and groups more resilient to radicalization.	**FEMA NPD**	Curriculum Review - March 2016. Anticipated Availability - June 2016. Target audience: Community Liaison Officers, School Resource Officers, NGOs and community leaders.

Management and planning level online training for state, local, tribal and territorial Community Liaison Officers, School Resource Officers, NGOs and community leaders. **This online course will provide an opportunity for participants to apply design thinking methodologies to develop community-based Countering Violent Extremism efforts.** - Community Based Prevention Approach to Violent Extremism. - Using Design Thinking to Address Violent Extremism. - Design Thinking Simulation: Introducing Empathy Research. - Design Thinking Simulation: Defining and Ideation Phases. - Design Thinking Simulation: Prototyping and Testing Phases. - Applying Design Thinking to Countering Violent Extremism in Your Own Community.	**FEMA NPD**	Curriculum Review - March 2016. Anticipated Availability – June 2016. Target audience: Community Liaison Officers, School Resource Officers, NGOs and community leaders.
Management and planning level course focuses on rural correctional facilities as unique breeding grounds for threat group recruitment and radicalization, examines the processes by which recruitment and radicalization occur, and proposes methods for strengthening the information gathering and sharing process. **This 8 hr. instructor led course address the following objectives:** - Describes the scope of gang, hate group, and terrorist group operations in rural jails and prisons. - Threat group member recruitment and radicalization in rural jails and prisons. - Effective information gathering and sharing among agencies. - An emphasis on the role of fusion centers, the Information. Sharing Environment and the Nationwide Suspicious Activity Reporting Initiative. - A focus on policy creation for radicalization and recruitment in rural jails and prisons.	**FEMA NPD**	Certified and approved course. Target audience: Rural detention officers, jailors, correction officers, public safety and law enforcement officers, fusion center intelligence analysts, correction facility decision makers.
Develop and deliver Strategic, Tactical, and Resilient		Funding

Interdiction of Violent Extremism (STRIVE), a collaborative, comprehensive, blended-learning national training program. STRIVE is designed to enhance the capacity and capabilities of communities to effectively counter violent extremism by fully integrating community policing principles into their CVE efforts. - The development of a comprehensive, blended-learning, two-day (16-hour) Strategic, Tactical, and Resilient Interdiction of Violent Extremism (STRIVE) national curriculum and Instructor Development Program (IDP); - Fifty-three (53) on-site STRIVE IDP courses (one in each state; and 3 pilots), training up to 50 participants per delivery, totaling 2,650 directly trained to implement STRIVE in their communities and to serve as a national cadre, each training 50 (est.) additional participants, totaling up to 132,500 community stakeholders trained nationwide; - Development and continuous delivery of the corresponding, technology-enhanced STRIVE Online Course, provided at no cost to a targeted 6,000 participants nationwide; - A STRIVE Online Resource Center, a web-based portal for program participants nationwide, to include: the course curriculum; technology and materials; the online course, the IDP track and report system; a promotional/marketing component (video trailer); and a best practices/lessons learned communications venue; and - One (1) Instructor Development Course (IDC), which will develop a cadre of twenty-five (25) nationally-certified STRIVE Instructors from multiple jurisdictions and multiple disciplines, to deliver this training on a national scope.	**FEMA NPD**	awarded September 2015. Anticipated Delivery – March 2017. Intended audience: Local government, law enforcement and all community stakeholders.
The National Consortium for the Study of Terrorism and Responses to Terrorism (START) proposes to develop a suite of five specialized training courses on Countering Violent Extremism (CVE). The courses target a range of community and government audiences engaged in mitigating and preventing violent extremism in local communities across the nation. While each course is designed as a stand-alone offering to fill a specific training gap, the full set offers a robust curriculum intended to increase expertise about CVE based on cutting-edge research and innovative training methodologies. - Just the Facts: Using Objective Data to Raise Community	**FEMA NPD**	Funding awarded September 2015. Anticipated Delivery – March 2017. The combined target audiences include representatives

Awareness about Violent Extremism: This 2-4 hour asynchronous online course will teach student to use dataset and knowledge tools maintained by START to raise community awareness of the behavioral, geographic and temporal characteristics of extremist violence at the state, local and national levels. - Integrating Mental Health and Education Approaches into CVE: This 2-4 hour asynchronous online course draws on the experience and capabilities present in the mental health and education fields and identifies areas of multidisciplinary collaboration and/or knowledge transfer within CVE practices and programs. - Countering Violent Extremist Narratives: Tools and Strategies: This 2-4 hour asynchronous online course introduces students to the spectrum of extremist narratives and their delivery mechanisms, as well as a spectrum of counter and alternate narratives and their respective development and delivery. - Designing Effective Rehabilitation and Reintegration Programs to Address Violent Extremism: This 2-4 hour asynchronous online course introduces rehabilitation and reintegration programming as an essential component of CVE efforts and teaches students in communities and institutional settings to design rehabilitation and reintegration programs. - Coalition Building for CVE and Community Resilience: This in person training will include 6 hours of content and provides a capstone hands-on simulation for students to gain experience with engagement, intervention, counter narrative and rehabilitation programming within a multidisciplinary team.		from NGOs, mental health professionals, law enforcement officers, analysts, and educators. Content will be designed to support coordination and cooperation across entities.

New Initiatives to Counter Violent Extremism

Enhance DHS collaboration with the technology and philanthropic sectors on CVE.
Enhance DHS efforts to counter the use of Internet and social media by violent extremists to radicalize individuals and groups to violence, recruit, and raise funds. Ensure that offline and online CVE activities are coordinated and leverage digital tools to increase effectiveness. Increase engagements with the private sector, including the technology, entertainment, marketing, and philanthropic sectors in support of online CVE efforts. Develop a digital implementation plan to both expand our outreach efforts online and incorporate emerging technologies and trends in social media, data analytics, and user experience design.

Implement a digital implementation plan that leverages technology to meet CVE goals. The digital engagement plan will identify and support innovative technology sector efforts to counter radicalization to violence and recruitment online; identify an approach to engage directly with technology companies to raise awareness of the violent extremist threat, ask them to identify ways to help counter violent extremism, and identify an approach to make critical information for individuals targeted by violent extremist organizations and their family and friends easily accessible online. – **Develop a structured outreach plan with relevant private sector entities:** – Hire Presidential Innovation Fellows to support CVE efforts: drawing on the President's newly-announced program to bring entrepreneurs, technologists and other innovators in to government, hire Fellows to join the CVE team to advise Department leadership and implement the digital implementation plan for CVE. – Utilize DHS Loaned-Executive program to provide executive-level talent from the private sector an opportunity to share their expertise with Homeland Security on CVE relevant programs and activities – Convene private sector leaders to solicit their input, identify best practices, and build collaborative efforts. – Increase collaboration with digital experts within government: Increase collaboration with the Office of Science and Technology Policy, US Digital Service, and other digital communication experts within government. – **Embed CVE within existing DHS activities to achieve scale and impact:** – Leverage existing USG internet safety campaigns: work with appropriate partners to integrate CVE into online and offline internet safety campaigns. – Leverage existing USG cybersecurity campaigns: work with appropriate partners to integrate information on terrorist use of the internet into existing departmental cybersecurity campaigns. – **Increase information-sharing with the American public.** – Ensure that information on violent extremism and responses is more accessible online: Rework the DHS	**OCP**	Digital plan is due by December 1, 2015. First quarterly update due January 2016.

    digital infrastructure to ensure that the public has access to useful and timely information on violent extremism, including information on terrorist groups, tactics, plots, radicalization, and interventions.

  - Provide threat briefings on violent extremism to tech sector partners: Develop concise and powerful materials to help technology sector leaders understand how violent extremists use the Internet and social media to radicalize, recruit, raise funds, and plan attacks.

  - Connect concerned parents and technology companies: work with technology companies and parents to create tools that help parents develop a better understanding of the online tools used by violent extremist organizations and become more aware of their children's activities online.

- **Create a robust environment to support private-sector led efforts online.**

  - Catalyze non-governmental initiatives to counter violent extremist activities online. Continue to support efforts such as Peer2Peer, which works with colleges and university around the world to incubate online CVE initiatives.

  - Identify government and private funding streams. Work with government and philanthropic partners to identify funding resources that can support both offline and online CVE initiatives.

  - Engage associations and professional bodies that advise and support national and local foundations and philanthropic entities to raise awareness of the threat of violent extremism and radicalization, as well as community-based efforts to implement prevention and intervention programs.

  - Support the development of incubators. Support the development of incubators that can support CVE initiatives, both offline and online from idea to scale.

  - Identify resources in the private sector to support online CVE initiatives. Reach out to the private sector, including the entertainment, marketing, and technology

sectors, to develop in-kind support networks for non-governmental CVE efforts. – **Develop government initiatives to counter violent extremists online.** – Support government initiatives to counter violent extremist narratives. Develop programs to counter violent extremist narratives online and deny their ability to use the internet and social media tools to radicalize to violence, recruit, raise funds, and plot attacks. – The digital implementation plan should include an engagement and outreach plan for the Secretary, the Deputy, and other Department senior leaders. The plan will include strategic objectives, a clear purpose and goal for each engagement and outreach activity, and a list of proposed partners (to include individuals and entities whose programs could be amplified, and organizations and institutions who could be helpful partners). – The implementation plan should also include an assessment plan to evaluate the impact and effectiveness of these efforts in coordination with S&T. – Provide quarterly updates detailing progress, lessons learned, and upcoming milestones or targets.		
Convene foundations, philanthropies, other private sector partners, and community-based CVE program leaders to discuss ways to collaborate to counter violent extremism. - Develop a philanthropic engagement plan that supports their efforts to stem recruitment and radicalization. - By November 1st, provide a calendar of FY16 proposed philanthropic engagements in specific communities. - For each engagement, identify: recommended DHS senior leader participants; regionally-specific goals and objectives; community-based programs we want to highlight; organizations and institutions who could be helpful partners (including U.S. Attorneys' Offices in those cities where the U.S. Attorney has engaged in community outreach to counter violent extremism); and recommended post-engagement actions. - Provide quarterly updates detailing progress, lessons learned, and recommendations for future engagements.	**OCP**	Philanthropic Engagement Plan and the Fiscal Year 2016 calendar of proposed philanthropic engagements are due by November 1, 2015. First quarterly update due January 2016.

Enhance DHS mechanisms for providing financial assistance to CVE programs. Strengthen our ability to support effective actions to counter violent extremism by expanding funding opportunities for community-based CVE programs.		
Improve DHS funding mechanisms for CVE. - Ensure that grant opportunities for CVE-related efforts and application processes are accessible and user-friendly for communities. - Explore ways to promote use of the Homeland Security Grant Program to support community-based programs. - Explore ways to promote use of the Nonprofit Security Grants Program for CVE-related uses. - In coordination with the Office for Community Partnerships, identify FY16 activities (including the CREX) that can be offered to CVE stakeholders as grant allowable resources and identify existing FEMA programs that can be leveraged for CVE related support. - Work with the Office for Community Partnerships, the DHS Office of Legislative Affairs and the Office of Management and Budget to explore a stand-alone CVE funding program and explore Secretarial discretionary funding options. - Work with the Office for Community Partnerships and the Office of Intergovernmental Affairs to reach out to Governors across the country to raise awareness on CVE priorities. - Building on the evaluation toolkit referenced below, enhance accountability and impact measurement of DHS-funded CVE programs. - Within 45 days, provide an interim progress report on these actions. - Provide quarterly updates detailing progress in meeting these goals.	**FEMA**	Initial plan due by October 5, 2015. Interim progress report due 45 after delivery of the initial plan. First quarterly update due January 2016.
Provide tools to our partners. Develop and field tools to help our state, local, tribal, and territorial government and community partners evaluate the impact of their CVE programs and to support effective interventions.		
Develop and field a program evaluation toolkit. - Develop and field a program evaluation toolkit to help our state, local, tribal, and territorial government and community partners evaluate the impact of their CVE	**S&T** **OCP**	Launch the research project by September 30, 2015.

programs. The toolkit should help community leaders identify measures to evaluate the impact of their efforts, and offer guidance on how to analyze and use evaluation data to improve their CVE programs. - (Development of these metrics is described in Line of Effort 3, page 16) (S&T) - Within 9 months of the research launch date, the toolkit should be made available to community partners. (OCP) - Report back on the lessons learned from the toolkit pilot testing within 18 months of the research launch date. (OCP)		Metrics delivered to DHS within 6 months. Toolkit fielded to partners within 9 months. Lessons learned reported within 18 months.
Develop and field screening tools to support effective intervention. - Develop tools to assist clinicians and others in referring individuals to intervention, treatment, and rehabilitation programs. - By November 30, 2015, fund the research project. (S&T, in partnership with DOJ) - Within 11 months of the research launch date, researchers will deliver tools to help determine whether individuals are suited for particular intervention programs. (S&T) - Within 12 months of the research launch date, DHS will make toolkits available to community-based mental health and counseling providers and others who might recommend an individual for an intervention program. (OCP) - Within 18 months of the research launch date, report back on the lessons learned from use of these tools. (OCP)	**S&T** **OCP**	Launch the research project by September 30, 2015. Tools delivered to DHS within 11 months of award. Toolkit fielded to partners within 12 months of award. Lessons learned reported within 18 months of award.
Improve and expand DHS field-based community engagement presence. Convene community stakeholders to build trust, identify capability and resource gaps, and facilitate capacity-building opportunities.		
Collaborate with federal partners to support field-based community engagement efforts to counter violent extremism. - Expand DHS support to the existing field-based community engagement programs by placing at least five full-time personnel in the first-tier cities to work in collaboration	**OCP**	Develop a plan to expand DHS field-based community engagement

with U.S. Attorneys' Offices and federal and local stakeholders in the area. - Draft supporting documentation for program management. These documents should specify component assignment criteria roles and responsibilities, budget and resourcing requirements (including a hiring plan), training requirements, and reporting chains (to both DHS headquarters and the local U.S. Attorneys' Offices). - Draft a template memorandum of understanding between DHS and each U.S. Attorney's Office to clarify the authorities, responsibilities, and reporting chains of DHS personnel in each USAO jurisdiction. - Provide quarterly updates detailing progress, lessons learned, and upcoming milestones or targets, including recommendations on how DHS can support community-based interagency CVE efforts more effectively.		presence due in 60 days. Draft documentation and hiring plan to expand DHS presence in the first-tier three cities due in 60 days. First quarterly update due January 2016.

2. Build trust and partnerships between government entities and communities.

DHS strives to maintain the public's trust and build partnerships with communities across the country. These efforts are wide-ranging and focus on all homeland security missions. However, these activities are essential to the Department's success in countering the violent extremist threat.

FOUNDATIONAL ACTIVITIES

DHS will work to build trust through our **routine community engagement**. Through the Office for Civil Rights and Civil Liberties (CRCL) Community Engagement Program, DHS conducts **community engagement roundtables** in more than 16 cities across the country every quarter. We are listening to community concerns, sharing our efforts to address those concerns, and ensuring that we are respecting individual rights in our day-to-day activities. CRCL does this every day in their many regular community engagements around the country, as do thousands of our DHS colleagues whose operational work touches the public every day.

DHS will also continue to assist in **coordinating federal engagement** in the immediate aftermath of an attack or incident of national significance to aid affected communities and to address follow-on concerns such as community backlash, safety, and the prevention of future attacks.

NEW INITIATIVES TO COUNTER VIOLENT EXTREMISM

Through the **"Your Homeland Security" campaign**, DHS will engage communities across the country, both online and offline, in a dialogue on how the Department can better serve their needs and how communities can help to keep the Homeland secure. Building upon ongoing activities such as DHS town hall meetings, this campaign will serve as a mechanism to increase awareness about DHS, expand discussion of community experiences and perceptions of DHS programs and policies, and enhance unity of effort between DHS and communities in achieving homeland security goals.

Both through their day-to-day efforts to serve the public and as members of their local communities, DHS employees play an important role in communicating our nation's values through what they say and do. The **"Every Interaction Counts" campaign** will increase DHS employee awareness of their critical role in demonstrating DHS' commitment to these values through their everyday actions, and through this campaign the Department recognizes the exemplary work of DHS employees in demonstrating these values.

DHS Actions to Counter Violent Extremism

2. Build trust and partnerships between government entities and communities.

Activity and Milestones	Lead Office	Target Date
FOUNDATIONAL ACTIVITIES		
Build trusted relationships to support community-based efforts. - Develop and maintain trusted relationships between the government and communities, including educators, parents, religious leaders, and private sector by hosting Community Engagement Roundtables, Youth Roundtables, the Secretary's Roundtables, and Community Engagement Town Hall Meetings. - Within 60 days of the date of issuance of this Action Plan, provide a plan including the following: - A calendar of proposed community engagement roundtables and town halls in specific communities. - For each roundtable and town hall, identify regionally-specific goals and objectives, community-based programs we want to highlight, organizations and institutions that might be helpful partners and recommended post-engagement actions. - Strategic objectives: what we hope to accomplish through the roundtables and town halls, and how to capture what we have learned from these efforts. - Provide quarterly updates detailing progress, lessons learned, and upcoming milestones or targets.	CRCL	Community Engagement Roundtables and Town Halls: ongoing. Initial plan due in 60 days. First quarterly update due January 2016.
Facilitate rapid response in the wake of an event. - Coordinate federal engagement resources and facilitate follow-on federal engagement with communities in the aftermath of an attack or an incident of national significance. - Continue to field the Incident Community Coordination Team national conference call mechanism in response to an attack or an incident of national significance.	CRCL	Ongoing.

<table>
<tr><th colspan="3">NEW INITIATIVES TO COUNTER VIOLENT EXTREMISM</th></tr>
<tr><td colspan="3"><b>Launch the "Your Homeland Security" campaign</b>
<i>Target audience: the American public and local communities</i>
DHS will leverage existing community outreach efforts and expand these efforts to additional communities and online to promote a sense of shared responsibility in keeping the homeland secure.</td></tr>
<tr><td><b>Develop an online and in-person community outreach and engagement campaign</b> that builds upon the Secretary's community engagement efforts to foster dialogue about how DHS can better serve different communities, dispel myths and negative stereotypes about DHS, and enlist communities in helping to achieve homeland security goals. This effort will involve many different types of communities and will seek to build trust, awareness about DHS, and unity of effort among our partners. It will provide opportunities for multiple Components to conduct community engagements together. A mechanism for community feedback to inform DHS programmatic and operational decisions is essential to the success of this effort.
- Within 60 days, submit a plan for this campaign, which will be built in to existing DHS outreach and engagement efforts.
- Within 180 days, submit an assessment plan to evaluate the impact and effectiveness of this campaign in coordination with S&T.
- Provide quarterly updates detailing progress, lessons learned, and upcoming milestones or targets.</td><td><b>CRCL
OPA
S&T</b></td><td>Initial plan due in 60 days.
Assessment plan due within 180 days.
First quarterly update due January 2016.</td></tr>
<tr><td colspan="3"><b>Initiate the "Every Interaction Counts" campaign</b>
<i>Target audience: DHS workforce</i>
Develop a campaign to increase DHS employee awareness of their critical role in building trust among those that they serve.</td></tr>
<tr><td>Launch the "Every Interaction Counts" campaign to raise awareness.
- Within 90 days, identify recommended methods for increasing awareness among DHS employees of their role in building trust with customers. Options may include senior leadership messaging, posters, awards to recognize exemplary actions, or modifications to training programs.</td><td><b>MGMT</b></td><td>Initial plan due within 90 days.</td></tr>
</table>

3. Understand the threat of violent extremism and effective efforts to counter the threat.

Basic research to enhance our understanding of the violent extremist threat is essential to ensure that DHS activities to counter violent extremism, and those of our partners, are appropriately focused. In addition, we need to understand which activities are effective in countering the threat.

FOUNDATIONAL ACTIVITIES

Focusing on the wide variety of threats, DHS will continue to work with other federal agencies, universities and Centers of Excellence, and international entities to conduct research and analysis to provide a comprehensive understanding of violent extremism in the United States.

DHS will continue to engage with communities and state, local, tribal, and territorial governments to identify non-securitized partnerships and approaches that have been effective in local communities and will facilitate the timely exchange of best practices through the Homeland Security Information Network. DHS will also continue to leverage the expertise of international partners to inform U.S.-based efforts.

NEW INITIATIVES TO COUNTER VIOLENT EXTREMISM

To enhance our understanding of what efforts are effective in countering violent extremism, DHS will **support the comprehensive evaluation of current CVE programs**, including both community-based programs and DHS efforts to support these activities. DHS will develop and field a program evaluation toolkit for community-based CVE programs, evaluate the impact of first-tier programs in Boston, Los Angeles and Minneapolis, and examine opportunities to enhance the Department's ability to obtain feedback from our community-based partners.

DHS will support the identification and testing of promising new ways to counter violent extremism. DHS will **support research and analysis to identify effective methods of countering violent extremism**, to include effective counter-messaging strategies and efforts to address root causes of radicalization to violence. DHS will also support innovation in peer-centered programs to counter violent extremist narratives.

DHS will **ensure that our efforts to counter violent extremism are directly informed by our understanding of the threat.** To accomplish this goal, DHS will ensure that research findings inform of the Department's CVE programs, and that research findings are more accessible to those engaged in CVE efforts.

To increase the effectiveness of our CVE programs in the face of a complex and rapidly-evolving threat, DHS will **ensure that research investments are prioritized to address critical CVE gaps** by developing research priorities that are informed by the needs of those directly engaged in CVE efforts.

DHS Actions to Counter Violent Extremism

3. Understand the threat and effective efforts to counter violent extremism.

Activity and Milestones	Lead Office	Target Date
FOUNDATIONAL ACTIVITIES		
Conduct focused research and analysis Support research and analysis to understand the threat of violent extremism.		
- Collect and catalog all U.S. Government-sponsored CVE- and counter-terrorism-related research and analysis projects and deliverables over the last five years. - Use empirical data and analysis to better understand the strategies violent extremist organizations use to recruit foreign fighters to Syria and Iraq, and to inspire homegrown terrorism. - Deliver the Terrorism and Extremist Violence in the United States (TEVUS) quantitative analytic dataset, a visual representation of extremist violence in the U.S. from 1970-present. - Conduct analysis to understand why some extremists leave the U.S. to become foreign fighters. - Deliver a report identifying patterns of mobilization and outcomes, using comparative case studies of returned individual foreign fighters. - Provide quarterly updates detailing progress, lessons learned, and upcoming milestones or targets.	S&T I&A	Catalog of sponsored research and analysis delivered within 18 months TEVUS delivered within 7 months Foreign fighter analysis delivered within 12 months. Report on patterns delivered within 17 months. First quarterly update due January 2016.
Engage communities and state, local, tribal and territorial entities to identify effective actions. Work with communities and state, local, tribal and territorial entities to identify CVE efforts that have been successful in local communities. Identify best practices from mental health, education, gang prevention, and other related fields that may be relevant for CVE prevention, intervention, and rehabilitation programming.		
- Through engagement, outreach, and DHS full-time support to local CVE efforts, identify best practices and facilitate exchange of ideas relating to CVE. - Provide an electronic forum for the timely exchange of CVE best practices through the Homeland Security	OCP S&T	Outreach and engagement: ongoing. First quarterly update due

Information Network. - Convene CVE grant awardees to share insights on effectiveness derived from DHS-funded community-based CVE programs. - Provide quarterly updates detailing progress, lessons learned, and upcoming milestones.		January 2016.
Leverage insights from international partners to supplement the threat picture in the United States and identify CVE best practices.		
- Continue to work with foreign governments, international law enforcement organizations and international CVE experts to identify best practices in other countries, ensuring that each engagement advances a clear purpose and set of goals. (OCP-S&T) - Exchange threat information and analysis with foreign governments and pursue joint analytic production opportunities. (I&A-CTC) - Complete the International CVE Roadmap, an analysis and report of outcomes for multinational long-term R&D engagement. (S&T) - Provide quarterly updates detailing progress, lessons learned, and upcoming milestones or targets. (OCP)	**OCP** **I&A** **S&T**	Outreach and engagement: ongoing. First quarterly update due January 2016.

New Initiatives to Counter Violent Extremism

Support the comprehensive evaluation of current CVE programs.
Develop tools to measure the effectiveness of community-based CVE programs. Evaluate current CVE programs to identify specific programs and methods that are effective in countering violent extremism.

Develop and field a program evaluation toolkit. - Develop and field a program evaluation toolkit to help our state, local, tribal, and territorial government and community partners evaluate the impact of their CVE programs. The toolkit should help community leaders select measures to evaluate the impact of their efforts, and offer guidance on how to analyze and use evaluation data for program improvement. - Launch and oversee a focused federally-funded R&D center project to develop the toolkit. - Provide monthly updates detailing progress in developing this toolkit. - A full set of metrics should be delivered to the Department within 6 months of the research launch date. - (Fielding and testing of these metrics is described in Line of Effort 1, page 7)	**PLCY**	Launch the research project no later than September 30, 2015. First monthly update due November 2015. Metrics delivered to DHS within 6 months.
Evaluate the outcomes and impacts of First-Tier programs in Boston and Los Angeles. - Award up to three grants to support assessment of the first-tier programs in Boston, Los Angeles or Minneapolis. - Publish notice of grant-making by September 1, 2015. - Award up to three grants by September 30, 2015. - Outcome measures for use in the evaluations are due four months from the date of the grant awards. - Assessments of the impact of the CVE programs are due 24 months from the date of the grant awards.	**S&T**	Publish notice of grant-making by September 1, 2015. Award up to three grants by September 30, 2015. Metrics due 4 months from date of awards. Impact evaluation due 24 months from date of awards.
Examine ways to assess community CVE program effectiveness.	**OGC**	Recommend-ations due within 60 days.

- Develop a recommendation to enhance the Department's ability to survey communities to assess CVE program effectiveness, consistent with the Paperwork Reduction Act of 1995.		
Encourage the identification and testing of new ideas for CVE Identify and test new methods of countering violent extremism.		
Support research and analysis to identify effective methods of countering violent extremism, to include: - Efforts to leverage resources and expertise resident in communities (e.g. mental health and anti-gang programs, faith-based organizations and educational institutions) to address root causes and intervene in potential cases of radicalization to violence. - Effective messaging (both content and means of delivery) to counter violent extremist narratives. - Conduct operational experiments for efficacy in meeting department and interagency CVE goals.	**S&T**	Initial plan due within 90 days.
Support private sector and youth-led innovation - Support opportunities (including incubators and University-led challenges) for CVE subject-matter experts and innovators from multiple disciplines to generate and share new ideas for countering violent extremism. - Expand DHS support of the Peer-to-Peer (P2P): Challenge Extremism program to further the design, testing, and implementation of P2P social and digital initiatives, projects and tools. - Support collaboration between academic institutions and students to counter violent extremism of all forms. - Within 90 days, submit a plan identifying potential partners, specific goals and milestones. The plan must include specific objectives, a clear purpose and goal for each engagement, and a list of proposed partners (to include organizations and institutions that could be helpful). The plan should also include an assessment plan to evaluate the impact and effectiveness of these efforts. - Provide quarterly updates detailing progress, lessons learned, and upcoming milestones or targets.	**OCP**	Plan due in 90 days. First quarterly update due January 2016.

Ensure that research investments are prioritized to address critical CVE gaps. Ensure that research on the threat of violent extremism is useful, timely, and targeted to meet the needs of CVE subject-matter experts within DHS, other federal agencies, and state, local, tribal and territorial entities.		
- Establish an Integrated Product Team to identify capability, research and development gaps relating to our efforts to counter violent extremism, and to coordinate research and development in support of these efforts. The team will be led by the Director for Community Partnerships with executive-level support from S&T. - Within 45 days, assess whether research on the threat of violent extremism meets the needs of CVE subject-matter experts, and use the results of the assessment to shape future research. - Within 90 days, submit a research implementation plan for CVE-relevant research and analysis. (S&T, in consultation with OCP) - Ensure that proposals for conducting CVE research are reviewed by OCP to confirm their usefulness for target users of research findings. (S&T) - Provide quarterly updates detailing progress, lessons learned, and upcoming milestones or targets. (OCP)	**S&T** **OCP**	Integrated Product Team established by November 1, 2015. Assessment due by December 15, 2015. Research plan due January 2016. First quarterly update due January 2016.
Ensure that DHS CVE efforts are directly informed by our understanding of the violent extremist threat. Leverage up-to-date insights on the threat of violent extremism in Departmental decision-making processes that determine and shape DHS' activities to counter violent extremism.		
- Increase access to and awareness of research on the threat of violent extremism among CVE subject-matter experts within DHS, other federal agencies, and state, local, tribal, and territorial government entities to better inform operational decisions in the field. - Ensure that research findings and lessons learned from CVE research and programs are appropriately taken into account in CVE programmatic decision-making within DHS. - Within 90 days, submit a set of recommendations to increase access to and awareness of research findings in the field, and to ensure that findings are taken into account in CVE programmatic decisions.	**OCP** **I&A** **S&T**	- Recommend-ations due within 90 days.

4. Improve coordination and direction of DHS efforts to counter violent extremism.

DHS Actions to Counter Violent Extremism

4. Improve coordination and direction of DHS efforts to counter violent extremism.

Activity and Milestones	Lead Office	Target Date
NEW INITIATIVES TO COUNTER VIOLENT EXTREMISM		
Establish the Office for Community Partnerships. Establish and fully resource the Office for Community Partnerships.		
- Publish a DHS Directive and instruction for the Office for Community Partnerships (OCP) establishing its authorities and responsibilities. – Direct an annual OCP reporting requirement to the Secretary on DHS CVE activities and efforts to build community resilience. – Establish resource and staffing plans for OCP.	MGMT	No later than October 30, 2015.
- Institutionalize OCP within the Department. - Formally establish OCP in the Department's FY2017 budget. - Secure a budget line for OCP beginning in FY17.	MGMT	By December 2016.
Measure program impacts and effectiveness of DHS CVE programs and share this data with senior leaders.		
- Provide an annual report to the Secretary on DHS CVE activities and efforts to build community resilience. The report should include an assessment of progress in meeting milestones and targets set for the year and recommendations for the following year's CVE activities, milestones, and targets.	OCP	FY16 Annual Report due by October 31, 2016.
Leverage outside expertise through the Homeland Security Advisory Council.		
- Explore establishing a CVE-focused subcommittee of the Homeland Security Advisory Council. - Provide a recommendation within 30 days. - *If approved*: identify and recruit subcommittee members, draft a tasking memo from the Secretary, and convene the first subcommittee meeting by	OPE HSAC	Provide a recommendation within 30 days. *If approved*, convene the first subcommittee

December 1, 2015.		meeting by December 1, 2015.

From: SLTT Partner Engagement

Sent: Wednesday, July 06, 2016 2:06:47 PM

To: Fusion Center Directors; RISS Center; SL Partners; HS.SLIC

Cc: Field Ops (ALL); IA-PartnershipEngagement; PE.SLTT; OSLLE; DHS.IGA

Subject: 2016 Countering Violent Extremism (CVE) Grant Program

Auto forwarded by a Rule

Partners,

Last year, Secretary Johnson and the DHS Office for Community Partnerships identified the need to make direct awards to non-governmental organizations for community-based countering violent extremism (CVE) programs. Congress has also been supportive of this effort by appropriating $10 million specifically to support local CVE efforts.

Today, DHS announced the FY 2016 CVE grant program to promote community resilience against the threat of violent extremism.

The DHS Office for Community Partnerships is working closely with the Federal Emergency Management Agency to ensure funding is awarded to community-based programs that draw from a range of local partners—for example, educators, social service and mental health providers, faith leaders and public safety officials.

The notice of funding opportunity and application process is now open. For more information on how to apply please go here: www.dhs.gov/cvegrants.

For programmatic questions about the funding opportunity please reach out to:
(b) (6)

Thank you

THE DEPARTMENT OF HOMELAND SECURITY ANNOUNCES THE COUNTERING VIOLENT EXTREMISM GRANT PROGRAM

WASHINGTON—On Wednesday, July 6, 2016, Secretary of Homeland Security Jeh Johnson announced the Fiscal Year (FY) 2016 Countering Violent Extremism (CVE) Grant Program, with $10 million in available funds. This is the first federal assistance program devoted exclusively to providing local communities with the resources to counter violent extremism in the homeland.

"As I have said before, given the nature of the evolving terrorist threat, building bridges to local communities is as important as any of our other homeland security missions," said Secretary Johnson. "This new grant program is an important step forward in these efforts and reflects the Department's continued commitment to protect the homeland and uphold our values."

In addition to state, local and tribal governments, non-profit organizations and institutions of higher education are eligible to apply. These grants will help scale community-led initiatives across the country to address the evolving terrorist threat, including international and domestic terrorism. Specifically, funding will support training, community engagements, and activities that challenge violent extremist narratives used to recruit and radicalize individuals to violence.

The Department's efforts to partner with local communities are a central part of its CVE mission. These grants will empower local communities to provide resources to friends, families and peers who may know someone on the path toward violent extremism, encouraging community-based solutions to deter an individual well before criminal or terrorist action, which would require the attention of law enforcement.

This grant program was developed by the DHS Office for Community Partnerships in conjunction with the Federal Emergency Management Agency. The Office for Community Partnerships builds relationships with local communities and leads the Department's CVE mission, focusing efforts to find innovative ways to discourage violent extremism and undercut terrorist narratives.

For more information on the FY16 CVE Grant Program, visit www.dhs.gov and www.grants.gov.

(b)(6)

From: (b)(6), (b)(7)c
Sent: Thursday, December 15, 2011 12:49 PM
Subject: DHS Webpage Launched Focusing on the Department's Work on Countering Violent Extremism (CVE)
Attachments: SIP-final.pdf

From: Frome, (b) (6)
Sent: Thursday, December 15, 2011 12:43 PM
To: OSLLE
Subject: DHS Webpage Launched Focusing on the Department's Work on Countering Violent Extremism (CVE)

Department of Homeland Security Partners and Stakeholders,

On behalf of Assistant Secretary Louis F. Quijas, the Office for State and Local Law Enforcement (OSLLE) is pleased to announce that today DHS launched a new webpage to highlight the Department's work in Countering Violent Extremism (CVE), part of the Administration's whole-of-government effort as detailed in the Strategic Implementation Plan (SIP) for Empowering Local Partners to Prevent Violent Extremism in the United States. The page serves as a hub for information regarding DHS' CVE efforts for federal, state, and local partners to assist with CVE engagement. This webpage also provides information and resources in support of DHS's three-layered approach to CVE: 1) Better understanding the phenomenon of violent extremism; 2) Bolstering efforts to address the dynamics of violent extremism and strengthening relationships with those communities targeted for recruitment by violent extremists; and 3) expanding support for information-driven, community-oriented policing efforts.

To access the new webpage, see: www.dhs.gov/cve. The SIP is also attached to this email.

If you have any feedback or questions regarding the DHS CVE activities please contact the (b) (6)

Thank you for all you do to help keep our nation safe and secure.

Stay Safe.

S(
b
(b) (6)
(
b
Office for State and Local Law Enforcement (OSLLE)
United States Department of Homeland Security
(b) (6)

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

DECEMBER 2011

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SECURITY STAFF

Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States

> As a government, we are working to prevent all types of extremism that leads to violence, regardless of who inspires it. At the same time, countering al-Qa'ida's violent ideology is one part of our comprehensive strategy to defeat al-Qa'ida. Over the past 2½ years, more key al-Qa'ida leaders—including Usama bin Laden—have been eliminated in rapid succession than at any time since the September 11 attacks. We have strengthened homeland security and improved information sharing. Thanks to coordinated intelligence and law enforcement, numerous terrorist plots have been thwarted, saving many American lives.
>
> —*President Barack Obama, August 2011*

Law enforcement and government officials for decades have understood the critical importance of building relationships, based on trust, with the communities they serve. Partnerships are vital to address a range of challenges and must have as their foundation a genuine commitment on the part of law enforcement and government to address community needs and concerns, including protecting rights and public safety. In our efforts to counter violent extremism, we will rely on existing partnerships that communities have forged with Federal, State, and local government agencies. This reliance, however, must not change the nature or purpose of existing relationships. In many instances, our partnerships and related activities were not created for national security purposes but nonetheless have an indirect impact on countering violent extremism (CVE).

At the same time, this Strategic Implementation Plan (SIP) also includes activities, some of them relatively new, that are designed specifically to counter violent extremism. Where this is the case, we have made it clear. It is important that both types of activities be supported and coordinated appropriately at the local level.

Background

The President in August 2011 signed the *National Strategy for Empowering Local Partners to Prevent Violent Extremism in the United States* (National Strategy for Empowering Local Partners), which outlines our community-based approach and the Federal Government's role in empowering local stakeholders to build resilience against violent extremism.[1] It recognizes that, as the National Security Strategy from May 2010 highlights, "our best defenses against this threat are well informed and equipped families, local communities, and institutions." To support our overarching goal of preventing violent extremists and their supporters from inspiring, radicalizing, financing, or recruiting individuals or groups in the

[1] The National Strategy for Empowering Local Partners defines violent extremists as "individuals who support or commit ideologically motivated violence to further political goals."

United States to commit acts of violence, the Federal Government is focused on three core areas of activity: (1) enhancing engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals.

The SIP details how we are implementing the National Strategy for Empowering Local Partners. It explains our core objectives and sub-objectives; describes how activities by departments and agencies are aligned with these; lists planned activities that address gaps and expand efforts; and assigns Federal Government leads and partners for various actions. The SIP provides a blueprint for how we will build community resilience against violent extremism.[2] It does not address our overseas CVE efforts, other than ensuring we coordinate domestic and international activities.

Although the SIP will be applied to prevent all forms of violent extremism, we will prioritize preventing violent extremism and terrorism that is inspired by al-Qa'ida and its affiliates and adherents, which the 2010 National Security Strategy, the 2011 National Strategy for Counterterrorism, and the National Strategy for Empowering Local Partners identify as the preeminent security threats to our country. This is, however, a matter of emphasis and prioritization, and does not entail ignoring other forms of violent extremism. As the July 2011 terrorist attack in Norway underscored, free societies face threats from a range of violent extremists.

As the activities described in the SIP are executed, there will be major and long-lasting impacts:

- There will be platforms throughout the country for including communities that may be targeted by violent extremists for recruitment and radicalization into ongoing Federal, State, and local engagement efforts;
- The Federal Government will support that engagement through a task force of senior officials from across the government;
- Community-led efforts to build resilience to violent extremism will be supported;
- Analysis will increase in depth and relevance, and will be shared with those assessed to need it, including Governor-appointed Homeland Security Advisors, Major Cities Chiefs, Mayors' Offices, and local partners;
- Training for Federal, State, tribal, and local government and law enforcement officials on community resilience, CVE, and cultural competence will improve, and that training will meet rigorous professional standards; and
- Local partners, including government officials and community leaders, will better understand the threat of violent extremism and how they can work together to prevent it.

[2] The concept of "resilience" has applied to a range of areas such as emergency preparedness and critical infrastructure protection (e.g., the ability of financial markets, power suppliers, and telecommunications companies to withstand an attack or disaster and resume operations rapidly.) The National Security Strategy emphasized the importance of including individuals and communities in our approach to enhancing resilience. Both the National Strategy for Empowering Local Partners and the 2011 National Strategy for Counterterrorism expanded this concept to CVE, the latter explicitly stating, "We are working to bring to bear many of these capabilities to build resilience within our communities here at home against al-Qa'ida inspired radicalization, recruitment, and mobilization to violence."

The SIP outlines ongoing, as well as planned, activities to counter violent extremism, which will be accomplished through existing funding and by prioritizing within the resources available to relevant departments and agencies. Some of these activities are specific to CVE, while others address broader non-security policy objectives but may have an indirect effect on countering radicalization to violence. Because our efforts are threaded across a range of different missions, such as training, outreach, and international exchanges, the execution of the SIP will be impacted by funding for both security and non-security related activities.

Process for Developing the SIP

The Obama Administration continues to prioritize and stress the critical importance of CVE in the Homeland. Given the complexities of addressing this threat and the uniqueness of the operating environment in the United States, the Administration recognizes the potential to do more harm than good if our Nation's approach and actions are not dutifully considered and deliberated. Throughout this process, careful consideration was given to the rule of law and constitutional principles, particularly those that address civil rights and civil liberties. With those principles in mind, we noted that departments and agencies with domestically focused mandates have an array of tools and capabilities that can be leveraged to prevent violent extremism, though some have limited experience in the national security arena. This necessitated a deliberative and carefully calibrated approach with an extensive evaluative period to fully address their potential roles and participation, which for some entailed thinking outside their traditional mandates and areas of work.

After assessing how individuals are radicalized and recruited to violence in the United States, the Administration established an accelerated process, led by the National Security Staff (NSS), to develop the National Strategy for Empowering Local Partners and the SIP. An Interagency Policy Committee (IPC) on countering and preventing violent extremism in the United States was established—with Assistant and Deputy Assistant Secretary-level representatives from across government—to consider roles and responsibilities, potential activities, guiding principles, and how best to coordinate and synchronize our efforts. The IPC, with support from specialist sub-IPCs, drafted our first national strategy on preventing violent extremism in the United States, which was approved by Deputies from the various departments and agencies and signed by the President.

- The following departments and agencies were involved in the deliberations and approval process: the Departments of State (State), the Treasury, Defense (DOD), Justice (DOJ), Commerce, Labor, Health and Human Services (HHS), Education (EDU), Veterans Affairs, and Homeland Security (DHS), as well as the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC).

To develop the SIP, the NSS tasked NCTC with coordinating the first comprehensive baseline of activities across the United States Government related to countering and preventing violent extremism in the United States, which constitutes the ongoing activities outlined in the SIP. This included CVE-specific initiatives, as well as activities that were not developed for CVE purposes, but nonetheless may indirectly contribute to the overall goals of the National Strategy for Empowering Local Partners. These activities were aligned with objectives and sub-objectives—based on the strategy and approved by the IPC—to

assess our overall effort and identify gaps. The IPC then considered ongoing and potential actions to address these gaps, which form the basis of planned activities outlined in the SIP. The SIP was approved by Deputies from the various departments and agencies in November 2011.

Compliance with the Rule of Law

A fundamental precept of the SIP is that the Federal Government's actions must be consistent with the Constitution and in compliance with U.S. laws and regulations. Departments and agencies are responsible for identifying and complying with legal restrictions governing their activities and respective authorities. Compliance with the rule of law, particularly ensuring protection of First Amendment rights, is central to our National Strategy for Empowering Local Partners and the execution of the SIP.

Crosscutting and Supportive Activities

There are fundamental activities that are critical to our success and cut across the objectives of the SIP. These include: (1) whole-of-government coordination; (2) leveraging existing public safety, violence prevention, and community resilience programming; (3) coordination of domestic and international CVE efforts, consistent with legal limits; and (4) addressing technology and virtual space. In many instances, these crosscutting and supportive activities describe the ongoing activities of departments and agencies in fulfilling their broader missions. As they implement new initiatives and programs in support of the SIP, departments and agencies will ensure these enabling activities appropriately guide their efforts.

1. Whole-of-Government Coordination

Leveraging the wide range of tools, capabilities, and resources of the United States Government in a coordinated manner is essential for success. Traditional national security or law enforcement agencies such as DHS, DOJ, and the FBI will execute many of the programs and activities outlined in the SIP. However, as the National Strategy for Empowering Local Partners states, we must also use a broader set of good governance programs, "including those that promote immigrant integration and civic engagement, protect civil rights, and provide social services, which may also help prevent radicalization that leads to violence." To this end, agencies such as EDU and HHS, which have substantial expertise in engaging communities and delivering services, also play a role.

This does not mean the missions and priorities of these partners will change or that their efforts will become narrowly focused on national security. Their inclusion stems from our recognition that radicalization to violence depends on a variety of factors, which in some instances may be most effectively addressed by departments and agencies that historically have not been responsible for national security or law enforcement. These non-security partners, including specific components within DOJ and DHS, have an array of tools that can contribute to this effort by providing indirect but meaningful impact on CVE, including after school programs, networks of community-based organizations that provide assistance to new immigrants, and violence prevention programs. We will coordinate activities, where appropriate, to support the CVE effort while ensuring we do not change the core missions and functions of these departments and agencies.

2. Leveraging Existing Public Safety, Violence Prevention, and Resilience Programming

While preventing violent extremism is an issue of national importance, it is one of many safety and security challenges facing our Nation. As we enter an era of increased fiscal constraints, we must ensure our approach is tailored to take advantage of current programs and leverages existing resources. Our efforts therefore will be supported, where appropriate, by emphasizing opportunities to address CVE within available resources related to public safety, violence prevention, and building resilience.

3. Coordination of Domestic and International Efforts

While always ensuring compliance with applicable laws and regulations, we must ensure a high level of coordination between our domestic and international efforts to address violent extremism. Although both the National Strategy for Empowering Local Partners and the SIP specifically address preventing violent extremism in the United States, the delineation between domestic and international is becoming increasingly less rigid. Violent extremists operating abroad have direct access to Americans via the Internet, and overseas events have fueled violent extremist radicalization and recruitment in the United States. The converse is also true: events occurring in the United States have empowered the propaganda of violent extremists operating overseas. While making certain that they stay within their respective authorities, departments and agencies must ensure coordination between our domestic and international CVE efforts. Given its mandate to support both domestic and international planning, NCTC will help facilitate this part of the CVE effort so that our Homeland and overseas activities are appropriately synchronized, consistent with all applicable laws and regulations. While individual departments and agencies will regularly engage foreign partners, all international engagement will continue to be coordinated through State.

4. Addressing Technology and Virtual Space

The Internet, social networking, and other technology tools and innovations present both challenges and opportunities. The Internet has facilitated violent extremist recruitment and radicalization and, in some instances, attack planning, requiring that we consider programs and initiatives that are mindful of the online nature of the threat. At the same time, the Federal Government can leverage and support the use of new technologies to engage communities, build and mobilize networks against violent extremism, and undercut terrorist narratives. All of our activities should consider how technology impacts radicalization to violence and the ways we can use it to expand and improve our whole-of-government effort. As noted in sub-objective 3.3, we will develop a separate strategy focused on CVE online.

Roles and Responsibilities

The SIP assigns Leads and Partners in each of the Future Activities and Efforts listed under respective sub-objectives. Leads and Partners have primary responsibility for coordinating, integrating, and synchronizing activities to achieve SIP sub-objectives and the overall goal of the National Strategy for Empowering Local Partners.

Expectation of Leads and Partners are as follows:

Lead: A department or agency responsible for convening pertinent partners to identify, address, and report on steps that are being taken, or should be taken, to ensure activities are effectively executed. The Lead is accountable for, among other things:

- Fostering communication among Partners to ensure all parties understand how to complete the activity;
- Identifying, in collaboration with assigned Partners, the actions and resources needed to effectively execute the activity;
- Identifying issues that impede progress; and
- Informing all departments and agencies about the status of progress by the Lead and other sub-objective Partners, including impediments, modifications, or alterations to the plan for implementation.

Partner: A department or agency responsible for collaborating with a Lead and other Partners to accomplish an activity. Partner(s) are accountable for:

- Accomplishing actions under their department or agency's purview in a manner that contributes to the effective execution of an activity;
- Providing status reports and assessments of progress on actions pertinent to the activity; and
- Identifying resource needs that impede progress on their department or agency's activities.

Assessing Progress

It is important to recognize that the National Strategy for Empowering Local Partners represents the first time the United States Government has outlined an approach to address ideologically inspired violent extremism in the Homeland. While the objectives and sub-objectives listed in the SIP represent the collective wisdom and insight of the United States Government about what areas of action have the greatest potential to prevent violent extremism, we will learn more about our effectiveness as we assess our efforts over time, and we will adjust our activities accordingly.

Given the short history of our coordinated, whole-of-government approach to CVE, we will first develop key benchmarks to guide our initial assessment. Where possible, we will also work to develop indicators of impact to supplement these performance measures, which will tell us whether our activities are having the intended effects with respect to an objective or sub-objective. As we implement our activities, future evaluations will shift away from benchmark performance measures towards impact assessments. Departments and agencies will be responsible for assessing their specific activities in pursuit of SIP objectives, in coordination with an Assessment Working Group. We will develop a process for identifying gaps, areas of limited progress, resource needs, and any additional factors resulting from new information on the dynamics of radicalization to violence. Our progress will be evaluated and reported annually to the President.

Objectives, Sub-Objectives, and Activities

The SIP's objectives mirror the National Strategy for Empowering Local Partners' areas of priority action: (1) enhancing Federal engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals. Each of these is supported by sub-objectives, which constitute measurable lines of effort with which our specific programs and initiatives are aligned. A key purpose of the SIP is to describe the range of actions we are taking to improve or expand these efforts.

1. Enhancing Federal Engagement with and Support to Local Communities that May be Targeted by Violent Extremists

Communication and meaningful engagement with the American public is an essential part of the Federal Government's work, and it is critical for developing local partnerships to counter violent extremism. Just as we engage and raise awareness to prevent gang violence, sexual offenses, school shootings, and other acts of violence, so too must we ensure that our communities are empowered to recognize threats of violent extremism and understand the range of government and nongovernment resources that can help keep their families, friends, and neighbors safe. As noted in the National Strategy for Empowering Local Partners:

> Engagement is essential for supporting community-based efforts to prevent violent extremism because it allows government and communities to share information, concerns, and potential solutions. Our aims in engaging with communities to discuss violent extremism are to: (1) share sound, meaningful, and timely information about the threat of violent extremism with a wide range of community groups and organizations, particularly those involved in public safety issues; (2) respond to community concerns about government policies and actions; and (3) better understand how we can effectively support community-based solutions.

At the same time, we must ensure that our efforts to prevent violent extremism do not narrow our relationships with communities to any single issue, including national security. This necessitates continuing to engage on the full range of community interests and concerns, but it also requires, where feasible, that we incorporate communities that are being targeted by violent extremists into broader forums with other communities when addressing non-CVE issues. While we will engage with some communities specifically on CVE issues because of particular needs, care should be taken to avoid giving the false impression that engagement on non-security issues is taking place exclusively because of CVE concerns. To ensure transparency, our engagement with communities that are being targeted by violent extremists will follow two tracks:

- We will specifically engage these communities on the threat of violent extremism to raise awareness, build partnerships, and promote empowerment. This requires specific conversations and activities related to security issues.
- Where we engage on other topics, we will work to include them in broader forums with other communities when appropriate.

1.1 Improve the depth, breadth, and frequency of Federal Government engagement with and among communities on the wide range of issues they care about, including concerns about civil rights, counterterrorism security measures, international events, and foreign policy issues.

Violent extremist narratives espouse a rigid division between "us" and "them" that argues for exclusion from the broader society and a hostile relationship with government and other communities. Activities that reinforce our shared sense of belonging and productive interactions between government and the people undercut this narrative and emphasize through our actions that we are all part of the social fabric of America. As President Obama emphasized, when discussing Muslim Americans in the context of al-Qa'ida's attempts to divide us, "we don't differentiate between them and us. It's just us."

Current Activities and Efforts

Departments and agencies have been conducting engagement activities based on their unique mandates. To better synchronize this work, U.S. Attorneys, who historically have engaged with communities in their districts, have begun leading Federal engagement efforts. This includes our efforts to engage with communities to (1) discuss issues such as civil rights, counterterrorism security measures, international events, foreign policy, and other community concerns; (2) raise awareness about the threat of violent extremism; and (3) facilitate partnerships to prevent radicalization to violence. The types of communities involved in engagement differ depending on the locations. United States Attorneys, in consultation with local and Federal partners, are best positioned to make local determinations about which communities they should engage. Appointed by the President and confirmed by the Senate, U.S. Attorneys are the senior law enforcement and executive branch officials in their districts, and are therefore well-placed to help shape and drive community engagement in the field.

In December 2010, 32 U.S. Attorneys' Offices began expanding their engagement with communities to raise awareness about how the United States Government can protect all Americans from discrimination, hate crimes, and other threats; to listen to concerns; and to seek input about government policies and programs. In some instances, these efforts also included initiatives to educate the public about the threat of violent extremist recruitment, which is one of many components of a broader community outreach program.

- During this initial pilot, these U.S. Attorneys significantly expanded outreach and engagement on a range of issues of interest to communities; built new relationships where needed; and communicated the United States Government's approach to CVE.
- Departments and agencies, including State, the Treasury, EDU, HHS, and DHS provided information, speakers, and other resources for U.S. Attorneys' community engagement activities, frequently partnering with DOJ on specific programs and events.

A National Task Force, led by DOJ and DHS, was established in November 2010 to help coordinate community engagement at the national level. It includes all departments and agencies involved in relevant community engagement efforts and focuses on compiling local, national, and international best practices and disseminating these out to the field, especially to U.S. Attorneys' Offices. The Task Force is also responsible for connecting field-based Federal components to the full range of United States Government officials involved in community engagement to maximize partnerships,

coordination, and resource-sharing. The following are some examples of engagement efforts that are, or will be, coordinated with the Task Force:

- The DHS Office for Civil Rights and Civil Liberties (CRCL) this year doubled its outreach to communities and expanded its quarterly engagement roundtables to 14 cities throughout the country. During Fiscal Year 2011, CRCL also conducted 72 community engagement events, some of which included CVE-related topics.
- State engaged on U.S. foreign policy with a range of interested domestic communities. The Bureau of Near Eastern Affairs alone conducted 80 outreach events over the past year.
- DOJ has produced a number of brochures and other materials on civil rights protections and steps individuals can take to prevent or respond to discrimination, and has disseminated these to various communities, including those being targeted by violent extremists. DOJ has translated these materials into a number of languages, including Arabic, Somali, Urdu, Farsi, and Hindi.
- DOJ, in coordination with DHS, expanded the Building Communities of Trust (BCOT) Initiative, which focuses on developing relationships among local law enforcement departments, fusion centers, and the communities they serve to educate communities on: (1) the Nationwide Suspicious Activity Reporting Initiative (NSI); (2) how civil rights and liberties are protected; and (3) how to report incidents in order to help keep our communities safe. DOJ continues to support the BCOT Initiative.

Future Activities and Efforts

The primary focus for the next year will be: (1) expanding the scope of engagement; (2) building new partnerships between communities and local law enforcement, local government officials, and civil society; (3) incorporating communities that are being targeted by violent extremist radicalization into broader forums with other communities to engage on a range of non-security issues; and (4) increasing our engagement specifically on CVE. Additional activities going forward include the following:

- DOJ will incorporate more U.S. Attorneys' Offices as engagement leads in the field, building on the initial U.S. Attorney-led effort. (Lead: DOJ; Partners: All)
- The National Task Force will: (1) disseminate regular reports on best practices in community engagement to local government officials, law enforcement, U.S. Attorneys' Offices, and fusion centers; (2) work with departments and agencies to increase their support to U.S. Attorney-led engagement efforts in the field; and (3) closely coordinate Federal engagement efforts with communities targeted by violent extremist radicalization. (Leads: DOJ and DHS; Partners: All)
- In consultation with Federal and local partners, the National Task Force and the U.S. Attorneys' Offices will facilitate, where appropriate, the inclusion of communities that may be targeted by violent extremist radicalization into broader engagement forums and programs that involve other communities. (Leads: DOJ and DHS; Partners: All)
- U.S. Attorneys will coordinate closely with local government officials, law enforcement, communities, and civil society to enhance outreach events and initiatives. (Lead: DOJ; Partners: All)

- In Fiscal Year (FY) 2012, CRCL plans on expanding its quarterly community engagement roundtables to a total of 16. CRCL is also in the process of implementing a campus youth community engagement plan, through which it will engage with young adults on the topic of violent extremism. (Lead: DHS)
- Depending on local circumstances, and in consultation with the FBI and other agencies as appropriate, U.S. Attorneys will coordinate any expanded engagement specific to CVE with communities that may be targeted by violent extremist radicalization. (Lead: DOJ; Partners: DHS, NCTC, and FBI)
- An FBI CVE Coordination Office will be established and, as part of its activities, will coordinate with the National Task Force on CVE-specific education and awareness modules. These modules will be developed and implemented, in part, by leveraging some of the FBI's existing programs and initiatives. (Lead: FBI; Partners: DOJ and DHS)
- DHS will oversee an online portal to support engagement by government officials and law enforcement with communities targeted by violent extremist radicalization, which will be used to share relevant information and build a community of interest. The portal will be accessible to government officials and law enforcement involved in overseas and domestic CVE and community engagement efforts to share best practices. (Lead: DHS; Partners: State, and NCTC)
- DOJ will expand the efforts of the BCOT initiative to help facilitate trust between law enforcement and community leaders. This dialogue could include local issues, as well as CVE. (Lead: DOJ; Partner: DHS)
- The United States Government will build a digital engagement capacity in order to expand, deepen, and intensify our engagement efforts. Where possible, virtual engagement will build on real world engagement activities and programs. (Lead: DHS; Partners: All)

1.2 Foster community-led partnerships and preventative programming to build resilience against violent extremist radicalization by expanding community-based solutions; leveraging existing models of community problem-solving and public safety; enhancing Federal Government collaboration with local governments and law enforcement to improve community engagement and build stronger partnerships; and providing communities with information and training, access to resources and grants, and connections with the philanthropic and private sectors.

The Federal Government can foster nuanced and locally rooted counter-radicalization programs and initiatives by serving as a facilitator, convener, and source of information to support local networks and partnerships at the grassroots level. Importantly, because the dynamics of radicalization to violence frequently vary from location to location, we recognize that a one-size-fits-all approach will be ineffective.

Current Activities and Efforts

The Federal Government has held a series of consultative meetings with communities, local government and law enforcement, civil society organizations, foundations, and the private sector to better understand how it can facilitate partnerships and collaboration. This leverages a key strength identified

in the National Strategy for Empowering Local Partners: "The Federal Government, with its connections to diverse networks across the country, has a unique ability to draw together the constellation of previously unconnected efforts and programs to form a more cohesive enterprise against violent extremism." Examples of this include the following:

- DHS Secretary Napolitano tasked her Homeland Security Advisory Council (HSAC) to develop recommendations on how the Department can best support law enforcement and communities in their efforts to counter violent extremism. An HSAC CVE Working Group convened multiple meetings with local law enforcement, local elected officials, community leaders (including faith-based leaders), and academics. The working group released its recommendations in August 2010, highlighting the importance of: (1) research and analysis of violent extremism; (2) engagement with communities and leveraging existing partnerships to develop information-driven, community-based solutions to violent extremism and violent crime; and (3) community oriented policing practices that focus on building partnerships between law enforcement and communities.
- DHS and NCTC began raising awareness about violent extremism among private sector actors and foundations and connected them with community civic activists interested in developing programs to counter violent extremism. DHS is now working with a foundation to pilot resiliency workshops across the country that address all hazards, including violent extremism.

We also began exploring how to incorporate CVE as an element of programs that address broader public safety, violence prevention, and resilience issues. This has the advantage of leveraging preexisting initiatives and incorporates CVE in frameworks (such as safeguarding children) used by potential local partners who may otherwise not know how they fit into such efforts. For example, although many teachers, healthcare workers, and social service providers may not view themselves as potentially contributing to CVE efforts, they do recognize their responsibilities in preventing violence in general. CVE can be understood as a small component of this broader violence prevention effort. Departments and agencies will review existing public safety, violence prevention, and resilience programs to identify ones that can be expanded to include CVE as one among a number of potential lines of effort.

- As an example, the Federal Government helped support a community-led initiative to incorporate CVE into a broader program about Internet safety. The program addressed protecting children from online exploitation, building community resilience, and protecting youth from Internet radicalization to violence.

Future Activities and Efforts

Planned activities to expand support to local partners include the following:

- The Federal Government will help broker agreements on partnerships to counter violent extremism between communities and local government and law enforcement to help institutionalize this locally focused approach. (Lead: DHS)
- DHS and DOJ will work to increase support for local, community-led programs and initiatives to counter violent extremism, predominantly by identifying opportunities within existing appropriations for incorporating CVE as an eligible area of work for public safety, violence prevention, and community resilience grants. (Leads: DHS and DOJ)

- DHS is working to increase funding available to integrate CVE into existing community-oriented policing efforts through FY12 grants. (Lead: DHS)
- DHS is establishing an HSAC Faith-Based Community Information Sharing Working Group to determine how the Department can: (1) better share information with faith communities; and (2) support the development of faith-based community information sharing networks. (Lead: DHS)
- DHS is developing its Hometown Security webpage to include resources such as training guidance, workshop reports, and information on CVE for both the general public and law enforcement. (Lead: DHS)
- The Treasury will expand its community outreach regarding terrorism financing issues. (Lead: Treasury; Partners: State, DOJ, DHS, FBI, and the U.S. Agency for International Development)[3]
- Depending on local circumstances and in consultation with the FBI, U.S. Attorneys will coordinate, as appropriate, any efforts to expand connections and partnerships at the local level for CVE, supported by the National Task Force where needed. (Lead: DOJ; Partners: All)
- Departments and agencies will expand engagement with the business community by educating companies about the threat of violent extremism and by connecting them to community civic activists focused on developing CVE programs and initiatives. (Lead: DHS; Partner: NCTC)

2. Building Government and Law Enforcement Expertise for Preventing Violent Extremism

It is critical that the Federal Government and its local government and law enforcement partners understand what the threat of violent extremism is, and what it is not. This helps ensure that we focus our resources where they are most effective and that we understand how we can best empower and partner with communities. Building expertise necessitates continued research about the dynamics of radicalization to violence and what has worked to prevent violent extremism; sharing this information as widely as possible; and then leveraging it to train government officials and law enforcement.

2.1 Improve our understanding of violent extremism through increased research, analysis, and partnerships with foreign governments, academia, and nongovernmental organizations.

The Federal Government has built a robust analytic program to understand violent extremism that includes analysis; research conducted by academia, think tanks, and industry; and exchanges with international allies to identify best practices. While we have increased our understanding of how individuals are radicalized to violence, we must continue to identify gaps, monitor changes in the dynamics of violent extremism, and remain vigilant by challenging our assumptions and continuing our research and analysis.

Current Activities and Efforts

The United States Government's research capacity on this issue has greatly expanded. DHS and NCTC both have analytic groups exclusively focused on violent extremist radicalization; the Interagency Intelligence Subcommittee on Radicalization helps coordinate and improve CVE intelligence analysis; and we work with foreign governments, academia, and nongovernmental organizations to inform and

[3] The U.S. Agency for International Development's role will be limited to sharing relevant information.

supplement our analysis and understanding. In addition to a large volume of intelligence products on CVE, examples of activities include:

- DHS Science & Technology (S&T) sponsored research on violent extremism in the United States, which it has shared with DHS components and other departments and agencies. Over 20 reports have been produced since 2009 and 5 more will be produced by the end of 2011. DHS is also developing an integrated open source database to help inform CVE programs.
- DHS's Office of Intelligence and Analysis (I&A) collaborated with the FBI, the Bureau of Prisons (BOP), and NCTC to assess the capacity of state correctional institutions to detect and share information regarding individuals who demonstrate behaviors associated with violent extremism while in the correctional system.
- The National Intelligence Council, DHS, FBI, and NCTC briefed fusion centers and law enforcement around the country on violent extremism.
- DHS, in partnership with the FBI and NCTC, developed case studies on preoperational indicators and known threats for State and local law enforcement and affected communities.
- The United States Government held regular exchanges of best practices with Australia, Canada, Denmark, Germany, the European Union, the Netherlands, the United Kingdom, and other partners to gain comparative insights about what might be effective in the Homeland.
- DHS expanded cooperation between the United States and Canada on CVE research and lessons learned.
- The United States Government participates in the Global Counterterrorism Forum's CVE Working Group.
- As directed in the Fort Hood Follow-on Review, DOD established the Force Protection Senior Steering Group. Among the Steering Group's duties is the coordination of non-traditional partners' activities within DOD (e.g., counterintelligence and behavioral health) to better understand how to identify and prevent all forms of violent extremism—not limited to al-Qa'ida-inspired extremism—within the military, including the potential use of DOD's extensive network of programs designed to support individuals who are potentially at risk of committing acts of violence against themselves, their families, or co-workers.

Future Activities and Efforts

Although we have a better understanding of the threat, there are gaps that need to be addressed through additional research and analysis. In this regard, we will:

- Expand analysis in five priority areas (Leads: DHS, FBI, NCTC, and State):
  1. The role of the Internet in radicalization to violence and how virtual space can be leveraged to counter violent extremism.
  2. Single-actor terrorism (so called "lone wolves"), including lessons learned from similar phenomena such as a school shooters.
  3. Disengagement from terrorism and violent extremism.

4. Non-al-Qa'ida related radicalization to violence and anticipated future violent extremist threats.
5. Preoperational indicators and analysis of known case studies of extremist violence in the United States.

- Continue DHS S&T's support for research on countering the threat of extremist violence. (Lead: DHS)
- Continue DHS collaboration with the FBI, the BOP, and NCTC to: (1) improve awareness of the risk of violent extremism in correctional systems; (2) enhance screening of new inmates to detect individuals associated with violent extremist organizations; (3) improve detection of recruitment efforts within the correctional environment; and (4) increase information sharing, as appropriate, with Federal, State, and local law enforcement about inmates who may have adopted violent extremist beliefs and are being released. (Lead: DHS; Partners: DOJ, FBI, and NCTC)
- Complete the creation of the FBI CVE Coordination Office to help assess and leverage existing Bureau efforts to better understand and counter violent extremism. (Lead: FBI)
- Build lines of research specifically to support non-security Federal partners. (Leads: DHS and NCTC; Partners: EDU and HHS)

2.2 Increase Federal Government information sharing with State, local, and tribal governments and law enforcement on terrorist recruitment and radicalization.

As we enhance our partnerships with State, local, and tribal governments and law enforcement to counter violent extremism, it is essential that we share our expertise and insights about the dynamics of radicalization to violence and what has worked to prevent it. This, in turn, will help our partners identify potential areas of collaboration with communities and other local actors.

Current Activities and Efforts

Examples include:

- Based on direction from the Office of the Director of National Intelligence (DNI), DHS led an effort to improve the analysis of homegrown violent extremism, including analytic tools to share with State, local, and tribal partners. DHS briefed representatives of 47 states on the project.
- DHS generated case studies of known and suspected terrorists and assessments of radicalization to violence, based on recent arrests, to share with local partners.
- FBI disseminated information to public safety partners, including information about radicalization to violence.
- DHS, NCTC, and FBI briefed and disseminated information on how individuals are radicalized to violence to law enforcement, fusion centers, and local government officials, including the Major Cities Chiefs, representatives from 47 states, Mayors' Offices, and State Homeland Security Advisors.

- In partnership with NCTC, DOJ, DNI, and FBI, DHS led the first National CVE Workshop in August 2011, which brought together intelligence commanders from major metropolitan areas and fusion center directors to increase their understanding of CVE.

Future Activities and Efforts

More work needs to be done to ensure our State, local, and tribal partners have the information they need to counter violent extremism. Classification remains an obstacle to broader sharing with these partners, but we can better ensure that analytic production is tailored to the needs of practitioners in the field. Major work over the next year will focus on creating more analytic products on CVE that directly support local law enforcement and government. Planned actions include:

- Development of an analytic team focused on supporting local government and law enforcement CVE practitioners and increased production of analysis at appropriate classification levels. (Lead: DHS; Partners: FBI and NCTC)
- Development of practitioner-friendly summaries of current research and literature reviews about the motivations and behaviors associated with single-actor terrorism and disengagement from violent extremism. (Lead: DHS)
- Review of information-sharing protocols to identify ways of increasing dissemination of products to State, local, and tribal authorities. (Leads: DHS, DOJ, FBI, and NCTC)
- Expansion of briefings and information sharing about violent extremism with State and local law enforcement and government. (Lead: DHS, FBI, and NCTC)

2.3 Improve the development and use of standardized training with rigorous curricula based on the latest research, which conveys information about violent extremism; improves cultural competency; and imparts best practices and lessons learned for effective community engagement and partnerships.

The Federal Government has expanded and improved training related to CVE over the past year, but challenges remain. In particular, there is a need for a review process and standards for training specific to CVE, which was underscored by a small number of instances of Federally sponsored or funded CVE-related and counterterrorism training that used offensive and inaccurate information, which was inconsistent with our values and core principles. As our National Strategy to Empower Local Partners highlights, "Misinformation about the threat and dynamics of radicalization to violence can harm our security by sending local stakeholders in the wrong direction and unnecessarily creating tensions with potential community partners." Therefore, improving Federal Government-approved training practices and processes related to CVE is a top priority of this plan.

Current Activities and Efforts

In November 2010, the IPC tasked DHS to form an Interagency Working Group on Training to catalogue and recommend improvements for CVE-related training across government. The Working Group brought together individuals responsible for CVE training and substantive specialists from civil rights and civil liberties offices, Federal law enforcement, and the analytic community. This is part of our overall

emphasis on improving the quality and quantity of CVE-related training. Notable accomplishments in our efforts to improve training include:

- Between October 2010 and October 2011, DHS CRCL trained nearly 2,700 law enforcement officials on CVE and cultural awareness at 46 separate events. The training served as the basis for best practices recommended by the Interagency Working Group on Training.
- Based on input from participating agencies, DHS issued CVE training guidance and best practices in October 2011 for Federal, State, local, and tribal government officials charged with organizing training related to CVE, cultural awareness, and counterterrorism.
- The Federal Emergency Management Agency (FEMA) in October 2011 issued an Information Bulletin on CVE Training, which includes DHS's training guidance and best practices, as well as guidance for State, local, and tribal entities that regularly leverage FEMA grants to fund CVE-related trainings. DHS sent the best practices paper and the FEMA guidance to all DHS grantees, State and local governments, State and local law enforcement, relevant community stakeholders, and interagency partners.
- DHS provided a full-day of training, which included training on cultural competency, civil rights, and civil liberties to Federal, State, local, and tribal partners at 12 fusion centers in the past year and over 30 fusion centers since 2008. These trainings were coupled with 3- to 4-hour CVE training sessions for State and local law enforcement operating in the same state. Additionally, DHS provided "train the trainer" sessions for staff from nearly all fusion centers nationwide.
- DHS, working closely with other departments and agencies, local law enforcement, academics, and curriculum development experts, developed guidelines for a CVE curriculum that focuses on information-driven community-oriented policing practices and how to leverage existing community partnerships to counter violent extremism and violent crime. These guidelines were reviewed and validated in February 2011 at a "proof-of-concept" session at the Federal Law Enforcement Training Center (FLETC), which was attended by State, local, and tribal law enforcement executives and frontline officers from rural and major city jurisdictions.
- State, working closely with NCTC and DHS, piloted specialized CVE training for United States Government officials working on CVE in the United States and abroad through its Foreign Service Institute in May 2011. Participation by domestic and international practitioners provided opportunities for exchanging best practices, enhanced the coordination of our Homeland and overseas efforts, and encouraged interagency partnerships.

Future Activities and Efforts

A review process by the Interagency Working Group on Training, as well as internal assessments by departments and agencies, indentified two key challenges, which we will address over the next year:

- Many departments and agencies lack a review process for training materials and outside speakers on CVE, which led to a small number of cases of training that violated internal principles as well as core tenets of the National Strategy to Empower Local Partners.

- There has been a lack of guidance and standards for training related to CVE, which left field offices, in particular, vulnerable to bad training. Without guidance or standards, it has been difficult to enforce accountability.

We have prioritized addressing these two shortcomings by doing the following:

- Departments and agencies are taking steps to identify training materials that may not meet internal standards and to improve processes for creating and reviewing such materials. Some departments are consulting with outside experts with established reputations to evaluate the content and training review process. Guidance on CVE-related training is being developed and will be issued, both across the organizations and to field components. Some departments may issue this as part of broader training guidance. (Lead: All)
- DHS, via FLETC, is in the process of developing a CVE curriculum to be integrated into existing training programs for Federal law enforcement. The curriculum will give Federal law enforcement a better understanding of CVE and how to more effectively leverage existing local partnerships. (Lead: DHS)
- DHS is in the process of establishing an internal committee to review all directly funded and issued DHS training on cultural competency, engagement, CVE, and counterterrorism. The committee will be responsible for reviewing any new content, evaluating experts, and establishing quality control. FEMA will incorporate the recently released Informational Bulletin and training guidance into FY12 grant guidance and will also leverage existing mechanisms to hold grantees and sub-grantees accountable. (Lead: DHS)

In addition to addressing the quality issue, we will work to expand the quantity of training.

- DHS, in partnership with the Los Angeles Police Department and the National Consortium for Advanced Policing, is developing a CVE curriculum that includes a 16-hour continuing education module for executive and frontline officers, as well as a 30-minute module that will be introduced at police academies. Both will be certified by the Police Officers Standards and Training Council. In October 2011 the Major Cities Chiefs Association passed a motion to adopt and implement the DHS CVE curriculum, which will be piloted with State and local law enforcement in San Diego by the end of 2011. By 2013, DHS seeks to: (1) implement the curriculum across the country on a regional basis; (2) develop a national network of trainers and subject matter experts who can administer the training and keep it current; and (3) build an online component for the curriculum. (Lead: DHS; Partners: DOJ and NCTC)
- DHS, via FLETC, will update current Federal training programs to integrate the CVE curriculum for Federal law enforcement in the coming year. (Lead: DHS)
- DHS is working with European law enforcement partners to share best practices and case studies to improve training, community policing, and operational information sharing. (Lead: DHS)
- DHS CRCL is expanding and institutionalizing its CVE and cultural competence training curricula to further enhance the material and its effectiveness. (Lead: DHS)

- The Interagency Working Group on Training will facilitate a "train the trainer program" to increase the reach of CVE training. (Leads: DHS and NCTC; Partners: DOJ, EDU, HHS, and FBI)
- The Interagency Working Group on Training will facilitate the development of an online training program that provides professional development credit for a broad range of professions, particularly those involved with public safety, violence prevention, and resilience. This will help build a basic understanding of CVE among a broad cross-section of stakeholders who have related mandates. (Leads: DHS and NCTC; Partners: DOJ, FBI, EDU, and HHS)
- The Interagency Working Group on Training will collaborate with non-security partners, such as EDU, to build CVE training modules that can be incorporated, as appropriate, into existing programs related to public safety, violence prevention, and resilience. These modules will be crafted in a way that is relevant to the specific audiences and their missions. Only trainers who have undergone CVE-specific training will deliver training programs that include CVE modules. (Lead: DHS; Partners: DOJ, EDU, HHS, FBI, and NCTC)
- DOD's training programs and curricula will be informed by the work of the Interagency Working Group on Training, as appropriate. Additionally, DOD is conducting a review of CVE-related curricula and will make revisions and adjustments as necessary. (Lead: DOD; Partner DHS)

3. Countering violent extremist propaganda while promoting our ideals

As the National Counterterrorism Strategy emphasizes, "[t]he United States was founded upon a belief in a core set of values that is written into our founding documents and woven into the very fabric of our society. Where terrorists offer injustice, disorder, and destruction the United States must stand for freedom, fairness, equality, dignity, hope, and opportunity. The power and appeal of our values enables the United States to build a broad coalition to act collectively against the common threat posed by terrorists, further delegitimizing, isolating, and weakening our adversaries."

Countering the ideologies and narratives that legitimize violence is central to our effort, but it also is the most challenging area of work, requiring careful consideration of a number of legal issues, especially those related to the First Amendment. In many instances, it will be more effective to empower communities to develop credible alternatives that challenge violent extremist narratives rather than having the Federal Government attempt to do so.

Our efforts include not only challenging justifications for violence, but affirming American ideals of inclusiveness and opportunity as well. Violent extremist narratives feed on disenchantment and the sense of exclusion. Our efforts therefore must include positive affirmation of our unity as a country. To some extent, this is addressed through our engagement activities, particularly where they address challenges facing all communities and not just those targeted by violent extremist radicalization. But there are also situations where we will need to more directly challenge violent extremist narratives.

3.1 Increase the capacity of communities to directly challenge violent extremist ideologies and narratives.

While the government cannot always directly contest violent extremist ideas, it can support capacity building within communities to take on this role. Whereas sub-objective 1.2 emphasizes preventative

measures and a defensive posture to build capacity for enhancing community resilience, sub-objective 3.1 focuses on increasing the ability of communities to push back against violent extremist propaganda.

Current Activities and Efforts

Most of our work in this area to date has focused on connecting community activists to potential civil society and private sector partners to focus specifically on undermining violent extremist narratives. Over the past year, we have taken the following steps:

- NCTC in 2010 developed a Community Awareness Briefing (CAB) to inform members of the public about efforts by al-Qa'ida and its adherents and affiliates to recruit Americans. The CAB highlights recruiting videos and examples of violent extremist propaganda, while underscoring the fact that these materials are often easily available on the Internet. Most importantly, the CAB aims to facilitate a discussion about what government and communities can do, together and independently, to counter the threat of violent extremist narratives. NCTC continues to deliver the presentation at forums composed of community leaders, educators, and parents in cities across the United States. In March 2011, NCTC held a workshop for local, State, and field-based Federal officials on how the CAB could be used in engagement efforts, when it makes sense and is appropriate.
- NCTC connected civic activists with technology experts, resulting in a training seminar on how to maximize the use of technology to counter violent extremism online.
- State sponsored speaker series and exchanges between international CVE practitioners and American communities targeted by violent extremist recruiters to better understand effective models for countering violent extremist narratives.

Future Activities and Efforts

This is a nascent area of effort and therefore will necessitate greater focus over the next year. Our planned actions include:

- Expanding efforts to raise community awareness about the threat of radicalization to violence, building from the experience of the CAB, and adapting those materials for different audiences where appropriate. (Leads: DOJ, DHS, FBI, and NCTC)
- Learning from former violent extremists, specifically those who can speak credibly to counter violent narratives, provide insights to government, and potentially catalyze activities to directly challenge violent extremist narratives. (Lead: DHS; Partner: NCTC)
- Providing grants to counter violent extremist narratives and ideologies, within authorities and relevant legal parameters, by reprioritizing or increasing the flexibility of existing funding. (Lead: DHS)
- Brokering connections between private sector actors, civil society, and communities interested in countering violent extremist narratives. (Lead: DHS; Partner: NCTC)
- Promoting international exchange programs to build expertise for countering violent extremist narratives. (Lead: State; Partners: DOJ, DHS, FBI, and NCTC)

- Increasing technical training to empower communities to counter violent extremists online, including the development of training for bloggers. (Lead: DHS; Partners: State, NCTC, and FBI)

3.2 Improve and increase our communication to the American public about the threat posed by violent extremist groups, myths and misperceptions about violent extremist radicalization, and what we are doing to counter the threat.

It is important that we communicate to the American public the realities of what the threat is, and what it is not. Misconceptions about the threat and statements and actions that cast suspicion on entire communities based on the actions of a few distract attention from the real threat and can undermine our ability to build partnerships. An informed citizenry enhances our national security.

Current Activities and Efforts

In 2011, the Federal Government focused on developing its approach to domestic CVE and communicating this to the American public. This involved briefings to Congress, public addresses, and media interviews. We will continue these activities.

Future Activities and Efforts

In 2012, we will work to expand our efforts to raise awareness in the general public about radicalization to violence in the United States and the tools to prevent it by:

- Providing regular briefings to Congress, think tanks, and members of the media. (Lead: DHS; Partners: DOJ, FBI, and NCTC)
- Creating programs to directly engage the public on the issue. (Lead: All)
- Building a public website on community resilience and CVE. (Lead: DHS)

3.3 Build a strategy to leverage new technologies and address online violent extremist radicalization

The Internet has become an increasingly potent element in radicalization to violence, enabling violent extremists abroad to directly communicate to target audiences in the United States. This direct communication allows violent extremists to bypass parents and community leaders. The SIP specifically addresses the online arena in several sub-objectives, but because of the importance of the digital environment, we will develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience that considers: (1) the latest assessment of the role of the Internet; (2) the absence of clear national boundaries in online space and the relationship between international and domestic radicalization to violence; (3) relevant legal issues; and (4) the differing authorities and capabilities of departments and agencies.

Conclusion

Protecting our Nation's communities from violent extremist recruitment and radicalization is a top national security priority. It is an effort that requires creativity, diligence, and commitment to our fundamental rights and principles. In his cover letter to the National Strategy for Empowering Local Partners, President Obama wrote:

> Sadly, the threat of violent extremism in America is nothing new. Throughout our history, misguided groups—including international and domestic terrorist organizations, neo-Nazis and anti-Semitic hate groups—have engaged in horrific violence to kill our citizens and threaten our way of life. Most recently, al-Qa'ida and its affiliates have attempted to recruit and radicalize people to terrorism here in the United States, as we have seen in several plots and attacks, including the deadly attack 2 years ago on our service members at Fort Hood. As a government, we are working to prevent all types of extremism that leads to violence, regardless of who inspires it.
>
> —President Barack Obama, August 3, 2011

A complex issue like violent extremist radicalization and recruitment requires a nuanced path to guide a whole-of-government approach. The SIP outlines this path and facilitates a division of labor by assigning responsibilities between Federal Government departments, agencies, and components focused on law enforcement and national security and those whose efforts support, but do not directly lie within, these areas.

From: FPS-INTEL
To: (b)(6), (b)(7)c

Subject: FW: QHSR TE Group - CT/CVE

From: (b) (6)
Sent: Tuesday, August 23, 2016 4:10:38 PM (UTC-05:00) Eastern Time (US & Canada)
To: (b) (6)

Subject: QHSR TE Group - CT/CVE
When:
Where: NAC 19-01-125

CT/CVE CHAPTER ONLY

Hi QHSR TE Group,

Most of you will not attend this meeting. Only one representative per Component Intelligence Program may attend; please decide among yourselves who can speak on behalf of your Component submissions and make decisions regarding the finality of text content. The ultimate attendee should have been involved in each step of the review thus far so that they are best informed as to the intent and direction of the content. Components without an interest in the Chapter are not required to attend; for everyone else, this is your last opportunity to impact this chapter substantively.

Please let me know by Friday noon if you are the chosen attendee. The entire group will still receive the new document version this Friday that we will discuss at the meeting.

Please let me know if you have any questions. Thanks and have a great day!
Best,
(b) a

(b) (6) .
Senior Intelligence Staff Officer
DHS CINT Staff
NAC 19-04-402-32
(b) (6)

From: FPS-INTEL
To: (b)(6), (b)(7)c
Subject: FW: State FY16 CT Partnership Fund Planning
Date: Tuesday, March 29, 2016 4:06:12 PM
Attachments: FOR DISCUSSION -- Updated State CTPF 16 Approach and Focus Areas (1).doc

From: Rohde, Brian
Sent: Tuesday, March 29, 2016 4:06:08 PM (UTC-05:00) Eastern Time (US & Canada)
To: CTAB Support SVTC; CTAB Dedicated POCS; CTAB Additional POCs
Cc: Taylor, Francis X; CT Staff; Blumenthal, Nathan; Ortiz, Louis
Subject: FW: State FY16 CT Partnership Fund Planning

All – the State Department notified DHS that it received $175 million for additional CT-related capacity building with foreign partners. State invited DHS to provide comments to the attached paper to identify priorities and focus areas for this specific appropriation.

PLCY send the formal tasking below through the Exec Sec process. I'm forwarding to the CT community to ensure your visibility. ***Comments are requested to Lou Ortiz and Brian Rohde by COB, Tuesday, April 5.***

Also, we're tentatively planning on a call Monday, April 4, 1:30 pm to discuss and go over any questions. Call bridge info to be provided later.

If you have any questions, please let me know.

Thanks.

Brian

Brian Rohde
Senior Advisor to the Counterterrorism Coordinator
U.S. Department of Homeland Security
(b) (6)

From: Ortiz, Louis
Sent: Tuesday, March 29, 2016 3:30 PM
To: (b) (6)

(b) (6)

Subject: State FY16 CT Partnership Fund Planning

All,

State CT received a $175M appropriation in the FY16 foreign operations budget and has initiated a strategic planning effort to coordinate programs and activities that may be funded through this and subsequent appropriations. They are seeking DHS input on the approach and focus areas. Attached is a planning document that State CT has drafted outlining program priorities, geographic/country areas of emphasis and potential budget breakout. They will be using this document to shape subsequent interagency planning and with stakeholders on the Hill, at Posts, and with our international partners. There will be additional coordination meetings, including select deep dives to discuss specific countries and subregions. They have asked for DHS to provide initial input on this document next week.

Accordingly, **NLT COB Tuesday, April 5,** please review and provide edits, comments and suggestions on the attached draft State CTPF 16 Approach and Focus Areas planning document. Please make specific recommendations on any changes to focus areas, priority for international partners and programs, and funding amounts with specific justification for any changes. Additionally, please note any additional information or coordination necessary to prepare subsequent plans or program recommendations including assessments, strategic planning guidance/plans, necessary resources, supporting engagements, or related program activities (i.e. overlap with training funded through other SSA appropriations).

DHS PLCY and CT Coordinator's Office will conduct a coordination phone call with component POCs tentatively **at 1330 on Monday, April 4, 2016** to coordinate DHS response to this request**.** DHS PLCY will provide dial in information to EXECSECS and designated component POCs.   CT Coordinator's Office will provide this to CTAB participants and provide updates as appropriate to highlight ongoing planning effort.

In responding, please respond directly to me and cc Brian Rhode. We will consolidate input and continue coordination of staff planning for program planning and implementation.

Lou Ortiz
Director, Asia-Pacific
Office of International Affairs
Department of Homeland Security

(b) (6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (6), (b) (5)