

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

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

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

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

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

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

Page 01 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

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

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 6 of 8

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

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

White House Summit to Counter Violent Extremism - Regional CVE Summits and Other Follow-On Initiatives

Dates	Organization	Host Entity	Location	Proposed Participants	WH Summit Workstreams or Elements of Action Agenda Covered	Notes
18-Apr	St. Paul Police Department	St. Paul Police Department	St. Paul, MN	Community leaders, local youth, law enforcement	2) Civil Society 3) Strengthening community-police relations	(b)(5)
29-Apr	DHS-CRCL	LinCT Conference	Los Angeles, CA	Law Enforcement Agencies, Experts, Criminal Justice Practitioners	3) Strengthening Community-Police Relations	
30-Apr	DOJ	US Attorney's Office - District of Massachusetts	Boston, MA	Researchers, criminal justice practitioners, service providers	2) Civil Society 5) Promoting Educational approaches	
7-May	DHS-CRCL	CRCL	New York, NY	Community Leaders, Civil Society Groups	1) Information Sharing 2) Civil Society	
8-May	DHS-CRCL	CRCL	Birmingham, AL	Community Leaders, Youth, Civil Society Groups	1) Information Sharing 2) Civil Society 4) Promoting Counter Narratives and Messaging	
May 11-13	DHS CRCL	State Department	London, UK	Community Leaders, Youth, Civil Society Groups	1) Information Sharing 2) Civil Society 4) Promoting Counter Narratives and Messaging	
May 12-13	DOJ	Community Oriented Policing Services (COPS) and the Police Executive Research Forum (PERF)	Washington, DC	Pilot sites, Montgomery County, law enforcement executives, community partners	2) Civil Society 3) Strengthening community-police relations	
23-May	St. Paul Police Department	St. Paul Police Department	St. Paul, MN	Community leaders, law enforcement, women in the community	2) Civil Society 3) Strengthening community-police relations	

27-May	DHS-CRCL	CRCL	Longmont, CO	Law Enforcement Agencies, Experts	3) Strengthening Community-Police Relations	(b)(5)
28-May	DOJ	US Attorney's Office - District of Colorado and FBI SAC	Denver, CO	Federal, state, and local government, law enforcement, social services, and mental health professionals	2) Civil Society 5) Promoting Educational approaches	
29-May	DHS-CRCL	CRCL/Local PD	Greeley, CO	Federal, state, and local government, law enforcement, social services, and mental health professionals	2) Civil Society 5) Promoting Educational approaches	
6-Jun	DHS-CRCL	CRCL	Scottsdale, AZ	Community Leaders, members, practitioners	2) Civil Society 5) Promoting Educational approaches	
June TBD	DOJ	US Attorney's Office - District of Massachusetts	Boston, MA	Community leaders and members, practitioners	2) Civil Society 4) Promoting the counter-narrative	
July 28-30	DOJ	National Institute of Justice (NIJ)& Department of Homeland Security (DHS) Science and Technology Directorate (S&T)	Washington, DC	Government representatives from the US, UK, and Canada, researchers, criminal justice practitioners	1) Promoting Local Research For Reference: CVE Summit Action Agenda Items: 1) Promoting Local Research and Information-Sharing on the Drivers of 2) Civil Society, including the Role of Women and Youth in Preventing and 3) Strengthening Community-Police and Community-Security Force Relations as Ingredients for Countering and Preventing Violent Extremism 4) Promoting the Counter-narrative and Weakening the Legitimacy of Violent Extremist Messaging 5) Promoting Educational Approaches to Build Resilience to Violent Extremism	

6) Enhancing Access to Mainstream Religious Knowledge
7) Preventing Radicalization in Prisons and Rehabilitating and Reintegrating Violent Extremists
8) Identifying Political and Economic Opportunities for Communities Vulnerable to Radicalization and Recruitment to Violent Extremism
9) Development Assistance and Stabilization Efforts to Prevent and Counter Violent Extremism



Countering Violent Extremism in the United States

Jerome P. Bjelopera
Specialist in Organized Crime and Terrorism

May 31, 2012

Congressional Research Service

7-5700

www.crs.gov

R42553

CRS Report for Congress

Prepared for Members and Committees of Congress

DHS-001-425-002530

Page 1 of 33

Summary

In August 2011, the Obama Administration announced its counter-radicalization strategy. It is devised to address the forces that influence some people living in the United States to acquire and hold radical or extremist beliefs that may eventually compel them to commit terrorism. This is the first such strategy for the federal government, which calls this effort “combating violent extremism” (CVE). Since the Al Qaeda attacks of September 11, 2001, the U.S. government has prosecuted hundreds of individuals on terrorism charges. Unlike the necessarily *secretive* law enforcement and intelligence efforts driving these investigations, the CVE strategy includes sizeable government activity within the *open marketplace of ideas*, where private citizens are free to weigh competing ideologies and engage in constitutionally protected speech and expression. Some of the key challenges in the implementation of the CVE strategy likely spring from the interplay between the marketplace of ideas and the secretive realm encompassing law enforcement investigations and terrorist plotting.

The strategy addresses the radicalization of all types of potential terrorists in the United States but focuses on those inspired by Al Qaeda. To further elaborate this strategy, in December 2011 the Administration released its “Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States” (SIP). The SIP is a large-scale planning document with three major objectives and numerous future activities and efforts. The SIP’s three objectives involve (1) enhancing federal community engagement efforts related to CVE, (2) developing greater government and law enforcement expertise for preventing violent extremism, and (3) countering violent extremist propaganda.

This report provides examples of recent Administration CVE activity and examines some of the risks and challenges evident in the SIP’s three objectives. The report also diagrams and briefly discusses the “future activities and efforts” outlined in the SIP for each of these three objectives. *A number of areas may call for oversight from Congress. These include the following:*

Picking Partners and Establishing “Rules of the Road”

Much of the federal government’s CVE effort centers on engagement with Muslim American community groups. This may not be as easy as simply reaching out to local organizations. Who speaks for diverse Muslim communities in America? What criteria will the Administration employ in its selection efforts, and how open will the process be? Once approved as partners, what “rules of the road” will govern continued cooperation? Ad hoc and opaque decision making might render the whole CVE outreach process arbitrary to some community participants. Congress may opt to consider whether there is a need to require the Administration to release public guidelines in this area.

Intervention with At-Risk Individuals

There appears to be little federally driven guidance to community groups on how to intervene with people vulnerable to radicalization. Congress may desire to require the Administration to examine the utility and feasibility of developing a CVE intervention model—possibly akin to gang intervention models—for the United States.

Identifying Programs to Assist Grassroots CVE Efforts

Working with communities entails informing them of possible resources they can use. A publicly available, comprehensive list of grant programs that can be harnessed for CVE activities does not exist. Congress may be interested in asking the Administration to formalize a roster or designate a clearinghouse available to local entities to identify such programs. By possibly pursuing this, Congress may help to ensure that local constituents have better information about and more direct access to federal CVE programs. On the other hand, such a list could be perceived as an additional layer of bureaucracy between constituents and grant programs.

Countering Extremist Ideas: Choosing Good vs. Bad

The task of countering extremist ideas highlighted in the CVE strategy and SIP raises a number of questions. Do the strategy and the SIP place the federal government in the business of determining which ideologies are dangerous and which are safe—essentially determining which beliefs are good and which are bad? In order to conduct effective oversight, Congress may choose to ask the Administration to define exactly what it means when referring to “violent extremist narratives.”

The Lack of a Lead Agency

There is no single agency managing all of the individual activities and efforts of the plan. At the national level, some may argue that it would be of value to have a single federal agency in charge of the government’s CVE efforts. From their perspective, without a lead agency it may be difficult to monitor the levels of federal funding devoted to CVE efforts and how many personnel are devoted to CVE in the federal government. For how many of these employees is counter-radicalization a full-time job? Are there mechanisms to track federal CVE expenditure? Which federal body is responsible for this? Congress may wish to pursue with the Administration the feasibility or value of designating a lead agency, or the possibility of naming a lead via legislation. However, it is unclear what types of authority—especially in the budgetary realm—such a lead may be able to wield over well-established agencies playing central roles in the CVE strategy.

Transparency

Without a high degree of transparency, an engagement strategy driven by federal agencies charged with intelligence gathering and law enforcement responsibilities may run the risk of being perceived as an effort to co-opt communities into the security process—providing tips, leads, sources, and informants. Some may maintain that this threatens to “securitize” a relationship intended as outreach within the marketplace of ideas. As such, critics may argue that it might not be particularly effective to have the same federal agencies responsible for classified counterterrorism investigations grounded in secrecy also be the main players in the CVE strategy. However, the Department of Homeland Security, the Department of Justice, and the Federal Bureau of Investigation have responsibilities for much of the CVE program. Because of this reality, Congress may opt to consider whether there is a need for greater transparency from the Administration in its CVE efforts.

Contents

Introduction: Counterterrorism Context	1
From Radicalization to Terrorism.....	3
Countering Radicalization in the United States	4
Administration Strategy and Current Activities	4
Community Engagement.....	5
Risks and Challenges	9
Building Government and Law Enforcement Expertise	14
Risks and Challenges	17
Countering Violent Extremist Propaganda.....	19
Risks and Challenges	19
Administration Plan and Future Activities	20
Is DHS the De Facto U.S. CVE Lead Agency?.....	20
Possible Policy Considerations for Congress	24
Implementing the CVE Strategy.....	24
Picking Partners and Establishing “Rules of the Road”.....	24
Intervention with At-Risk Individuals.....	25
Identifying Programs and Federal Contacts to Assist Grassroots CVE Efforts	26
Countering Extremist Ideas: Choosing Good vs. Bad.....	26
The Lack of a Lead Agency	27
Secretiveness vs. Transparency	28

Figures

Figure 1. Counterterrorism Context.....	2
Figure 2. Lead Agencies and Their “Future Activities and Efforts” for SIP Objective 1, <i>Enhancing Federal Engagement and Support to Local Communities that may be Targeted by Violent Extremists</i>	21
Figure 3. Lead Agencies and Their “Future Activities and Efforts” for SIP Objective 2, <i>Building Government and Law Enforcement Expertise for Preventing Violent Extremism</i>	22
Figure 4. Lead Agencies and Their “Future Activities and Efforts” for SIP Objective 3, <i>Countering Violent Extremist Propaganda While Promoting U.S. Ideals</i>	23

Contacts

Author Contact Information.....	29
---------------------------------	----

Introduction: Counterterrorism Context

In August 2011, the Obama Administration released its domestic counter-radicalization strategy. The Administration dubbed this effort “countering violent extremism” (CVE).¹ Implementation of the CVE strategy revolves around impeding the radicalization of violent jihadists in the United States.² As this may suggest, for this report, a couple of concepts are key. Namely, “radicalization” describes the process of acquiring and holding radical or extremist beliefs; and “terrorism” describes violent or illegal action taken on the basis of these radical or extremist beliefs.

This report examines the implementation of the Administration’s counter-radicalization strategy and provides possible policy considerations for Congress relating to this relatively new area of coordinated federal activity. Implementation of the CVE strategy involves many elements within the executive branch and brushes against a number of key issues involving constitutionally protected activity versus effective counterterrorism policing efforts.

Government-related efforts to stave off terrorist activity in the United States exist within two broad contexts. First, the operational aspects of violent terrorist plots largely involve clandestine illegal activity. Since the terrorist attacks of September 11, 2001 (9/11), hundreds of individuals have been implicated in more than 50 homegrown violent jihadist plots or attacks.³ In this *secretive realm*, law enforcement pursues terrorists in a real-world version of hide-and-seek. Domestic law enforcement strategies devised in the decade since 9/11 to prevent terrorism largely focus their efforts in this area.⁴ Federal law enforcement activity in this arena is geared toward rooting out terrorists and stopping them from successfully executing their plots.

¹ *Empowering Local Partners to Prevent Violent Extremism in the United States*, August 2011, p. 1, http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf. Hereinafter: *Empowering Local Partners*.

² The Obama Administration recognized the significance of the homegrown jihadist threat in its June 2011 *National Strategy for Counterterrorism*. This strategy document focuses on Al Qaeda, its affiliates (groups aligned with it), and its *adherents* (individuals linked to or inspired by the terrorist group). John Brennan, President Obama’s top counterterrorism advisor, publicly described the strategy as the first one, “that designates the homeland as a primary area of emphasis in our counterterrorism efforts.” See White House, *National Strategy for Counterterrorism*, June 2011, http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf; Mathieu Rabecchault, “U.S. Refocuses on Home-Grown Terror Threat,” *AFP*, June 29, 2011, <http://www.google.com/hostednews/afp/article/ALeqM5hLyJyB7khhqJxWOOlm1mCj7IYsRQ?docId=CNG.3f90005700ea65e0b05509a135c7a3a8.471>; Karen DeYoung, “Brennan: Counterterrorism Strategy Focused on al-Qaeda’s Threat to Homeland,” *Washington Post*, June 29, 2011, http://www.washingtonpost.com/national/national-security/brennan-counterterrorism-strategy-focused-on-al-qaedas-threat-to-homeland/2011/06/29/AGki1LrH_story.html.

³ See CRS Report R41416, *American Jihadist Terrorism: Combating a Complex Threat*, by Jerome P. Bjelopera. For lists of individuals involved in terrorism cases see <http://homegrown.newamerica.net/table>; “Profiles in Terror,” <http://motherjones.com/fbi-terrorist>. For this CRS report, “homegrown” describes terrorist activity or plots perpetrated within the United States or abroad by American citizens, legal permanent residents, or visitors radicalized largely within the United States. “Jihadist” describes radicalized Muslims using Islam as an ideological and/or religious justification for belief in the establishment of a global caliphate—a jurisdiction governed by a Muslim civil and religious leader known as a caliph—via violent means. Jihadists largely adhere to a variant of Salafi Islam—the fundamentalist belief that society should be governed by Islamic law based on the Quran and follow the model of the immediate followers and companions of the Prophet Muhammad. For more on Al Qaeda’s global network, see CRS Report R41070, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*, coordinated by John Rollins.

⁴ For more information on federal counterterrorism law enforcement, see CRS Report R41780, *The Federal Bureau of Investigation and Terrorism Investigations*, by Jerome P. Bjelopera.

The second context is the open *marketplace of ideas*. Here, private citizens are free to weigh competing ideologies and engage in constitutionally protected speech and expression. In this arena, a relative few ordinary law-abiding persons move from the mainstream and adopt radical ideologies that embrace terrorism. As they radicalize, *they do not necessarily commit crimes*. Much like the policing that occurs in the secretive realm, the federal government’s CVE strategy is a preventative approach to terrorism, *but it is not wholly focused on policing*. Rather, federal activity in this arena is geared toward helping local communities and individuals boost their resilience to terrorist radicalization efforts.

The divergent nature of these two contexts may imply clear distinction between the marketplace of ideas and the secretive operational realm. In reality, they are far from distinct. What happens operationally has significant impacts in the marketplace of ideas (**Figure 1**). This interrelationship is highlighted by any number of issues. For example,

- the success of terrorist plots in the secretive realm may spur radicalization and generate public fear in the marketplace of ideas;
- conversely, successful investigations in the secretive realm may discourage radicalizing individuals within the marketplace of ideas from eventually embracing violent acts of terrorism as an ultimate goal;
- effective policing within the secretive realm may depend on a trusting community acting supportively in the marketplace of ideas;
- perceived policing excesses in the secretive realm may impede community engagement with law enforcement; and
- high levels of radicalization occurring in the marketplace of ideas may expand the potential pool of terrorist recruits, while an effective government strategy to counter radicalization may staunch terrorist recruitment.

Figure 1. Counterterrorism Context



Source: CRS.

In fact, some of the key challenges involved in implementing a national strategy to deal with terrorist radicalization spring from the interplay between the marketplace of ideas and the secretive realm.

From Radicalization to Terrorism

A key way to fight the threat of homegrown terrorists is to develop an understanding of how radicalization works and formulate ways to prevent radicalization from morphing into terrorist plotting. In 2007, the New York City Police Department's (NYPD's) Intelligence Division released a study of domestic jihadist radicalization that has been widely circulated within the law enforcement community.

The NYPD study describes a general four-step process of radicalization leading to terrorist plotting. First, individuals exist in a pre-radicalization phase in which they lead lives unaware of or uninterested in either violent jihad or fundamentalist Salafi Islam. Next, they go through self-identification in which some sort of crisis or trigger (job loss, social alienation, death of a family member, international conflict) urges them to explore Salafism. Third, individuals undergo indoctrination or adoption of jihadist ideals combined with Salafi views. The study indicates that, typically, a "spiritual sanctioner" or charismatic figure plays a central role in the indoctrination process. Finally, radicalizing individuals go through "jihadization," where they identify themselves as violent jihadists, and are drawn into the planning of a terrorist attack.⁵ At this point, according to the NYPD, they can be considered violent extremists (terrorists). The Federal Bureau of Investigation's (FBI's) own four-stage model of radicalization closely follows that of the NYPD.⁶

This model and the process it describes—though useful—should, however, be read with caution, according to some observers. The radicalization process is best depicted in broad brush strokes. Brian Michael Jenkins has suggested that

There is no easily identifiable terrorist-prone personality, no single path to radicalization and terrorism. Many people may share the same views, and only a handful of the radicals will go further to become terrorists. The transition from radical to terrorist is often a matter of happenstance. It depends on whom one meets and probably on when that meeting occurs in the arc of one's life.⁷

Some experts have warned against viewing the radicalization process as a "conveyor belt," somehow starting with grievances and inevitably ending in violence.⁸ The NYPD report itself acknowledges that individuals who begin this process do not necessarily pass through all the stages nor do they necessarily follow all the steps in order, and not all individuals or groups who

⁵ Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, City of New York Police Department, Intelligence Division, New York, 2007, pp. 6-8, http://sethgodin.typepad.com/seths_blog/files/NYPD_Report-Radicalization_in_the_West.pdf. Hereinafter: Silber and Bhatt, *Radicalization in the West*.

⁶ Carol Dyer, Ryan E. McCoy, Joel Rodriguez, et al., "Countering Violent Islamic Extremism: A Community Responsibility," *FBI Law Enforcement Bulletin*, December 2007, p. 6.

⁷ Brian Michael Jenkins, *Would Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001* (Santa Monica, CA: The RAND Corporation, 2010), p. 7.

⁸ Sophia Moskalenko and Clark McCauley, "Measuring Political Mobilization: The Distinction Between Activism and Radicalism," *Terrorism and Political Violence*, vol. 21, no. 2 (April 2009), pp. 239-240.

begin this progression become terrorists.⁹ Studies by the Department of Homeland Security's (DHS's) Office of Intelligence and Analysis indicate that the radicalization dynamic varies across ideological and ethno-religious spectrums, different geographic regions, and socioeconomic conditions. Moreover, there are many diverse "pathways" to radicalization and individuals and groups can radicalize or "de-radicalize" because of a variety of factors.¹⁰

In a more fundamental conceptualization, radicalization expert Peter Neumann has noted that three core elements exist in the radicalization process. These are grievance, ideology/narrative, and mobilization.¹¹ Grievances can stem from narrow issues unique to an individual's personal life or arise from broader perceptions of the surrounding world. A radicalizing individual seizes upon extremist ideologies or narratives to help explain his or her grievance. Mobilization consists of an individual acting on his or her grievances based on precepts culled from a particular ideology or narrative. These actions can involve criminality.¹²

Countering Radicalization in the United States

Because so much of the radicalization process occurs within the marketplace of ideas, counter-radicalization efforts involve activity in the same realm. American counter-radicalization approaches favor government engagement with communities affected by terrorism. Scholars who have studied the circumstances that are associated with voluntary cooperation by Muslim-Americans in anti-terror policing efforts have identified strong evidence that when authorities are viewed as more legitimate, their rules and decisions are more likely to be accepted.¹³ Community engagement is—in part—an effort to make law enforcement authority more accepted within localities.

Administration Strategy and Current Activities

The Administration's CVE strategy revolves around countering the radicalization of all types of potential terrorists. As such, the radicalization of violent jihadists falls under its purview and is the key focus. The initial August 2011 strategy was supported by the Administration's release in December 2011 of its "Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States" (SIP).¹⁴ The SIP is a large-scale planning document with three major objectives and numerous future activities and efforts. There is no single lead agency

⁹ Silber and Bhatt, *Radicalization in the West*, pp. 10, 19.

¹⁰ U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, Written Testimony of Charles E. Allen, Assistant Secretary of Intelligence and Analysis and Chief Intelligence Officer, Department of Homeland Security, "Threat of Islamic Radicalization to the Homeland," 110th Cong., 1st sess., March 14, 2007, p. 5.

¹¹ Ryan Hunter and Danielle Heinke, "Radicalization of Islamist Terrorists in the Western World," *FBI Law Enforcement Bulletin*, (September 2011), pp. 27-29. <http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/september-2011>. Hunter and Heinke rely on the ideas of scholar Peter Neumann.

¹² *Ibid.*

¹³ Tom R. Tyler, Stephen Schulhofer, and Aziz Huq, "Legitimacy and Deterrence Effects in Counter-Terrorism Policing," New York University School of Law, Public Law Research Paper No. 10-15, February 23, 2010, p. 2, http://lsr.nellco.org/cgi/viewcontent.cgi?article=1182&context=nyu_plltpw.

¹⁴ *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States*, December 2011, <http://www.whitehouse.gov/sites/default/files/sip-final.pdf>. Hereinafter: *Strategic Implementation Plan*.

for any of the three objectives. Likewise, there is no single agency managing all of the individual future activities and efforts of the plan. The SIP's three objectives or "core areas of activity" are "(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 [U.S.] ideals."¹⁵

The following sections provide examples of recent Administration CVE activity and discussion of the risks and challenges evident in the SIP's three core areas of activity. The "future activities and efforts" outlined for each of the three core areas of activity in the SIP are also diagrammed and briefly discussed below.

Community Engagement

The concept of building trust through engagement and partnership is rooted in the community policing model developed by law enforcement professionals in the 1990s, and community policing is mentioned in the Administration's CVE strategy.¹⁶ Following the 9/11 attacks, law enforcement agencies came to realize the prevention of terrorist attacks would require the cooperation and assistance of American Muslim, Arab, and Sikh communities. "Embedded within these communities," notes Professor Deborah Ramirez, "are the linguistic skills, information, and cultural insights necessary to assist law enforcement in its efforts to identify suspicious behavior. In order to have access to these critical tools and information, law enforcement recognized the need to build bridges required for effective communication with these groups."¹⁷ At the same time, Muslim, Arab, and Sikh Americans recognized the need to define themselves as distinctly American communities who, like all Americans, desire to help prevent another terrorist attack.¹⁸

A study by the Homeland Security Institute found that "[c]ommunity policing has been applied with notable success in places such as New York City, Chicago, Boston, and San Diego, and has been widely adopted (at least in name) throughout the United States."¹⁹ A Homeland Security

¹⁵ Ibid., p. 2.

¹⁶ Ibid., pp. 3, 6. The Justice Department has defined community policing as "a philosophy that promotes organizational strategies, which support the systematic use of partnerships and problem-solving techniques, to proactively address the immediate conditions that give rise to public safety issues such as crime, social disorder, and fear of crime." One of its key features is the establishment of collaborative partnerships between law enforcement agencies and individuals and organizations they serve to develop solutions to problems and increase trust in police. See DOJ Office of Community Oriented Policing Services, *Community Policing Defined*, April 3, 2009, p. 3, <http://www.cops.usdoj.gov/files/RIC/Publications/c030917193-CP-Defined.pdf>.

¹⁷ Deborah A. Ramirez, Sasha Cohen O'Connell, and Rabia Zafar, *The Partnering for Prevention and Community Safety Initiative, A Promising Practices Guide Executive Summary*, 2004, p. 2, http://www.cps.neu.edu/plp/downloads/PPF_Executive_Summary__cover.pdf.

¹⁸ Ibid.

¹⁹ Rosemary Lark (Task Lead), Richard Rowe, and John Markey, *Community Policing Within Muslim Communities: An Overview and Annotated Bibliography of Open-Source Literature*. Homeland Security Institute, December 27, 2006, p. iii. This study, prepared for the DHS Science and Technology Directorate, sought to identify the literature that examined community policing initiatives underway within Muslim Communities in the U.S., and the extent to which they were successful in achieving the objectives of (1) inclusiveness, promoting integration, and potentially minimizing the disaffection that can lead to radicalization, particularly among Muslim youth; (2) serving as early warning to identifying incipient radicalization or terrorist activities; and (3) opening a new channel of communication with individuals who can navigate the linguistic and cultural complexities of Islam, providing needed context to inform intelligence analysis, http://www.homelandsecurity.org/hsireports/Task_06-99_Community_Policing_within_Muslim_Communities.pdf.

Advisory Council (HSAC) working group²⁰ chaired by Maryland Governor Martin O'Malley commented on Community-Oriented Policing, stating that

Effective public-private partnerships, designed to enable civic engagement, problem-solving, and violent crime mitigation provide the foundation for efforts to prevent, protect against and respond to violent criminal activity—including that which may be motivated by ideological objectives.²¹

The Administration's CVE strategy depends on federal agencies cooperating with local groups to expand engagement efforts and to foster preventative programming "to build resilience against violent extremist radicalization."²² In fact, it highlights a "community-based approach" for the federal government, and much of the activity it describes will take place in the "marketplace of ideas" described in **Figure 1**. To this end, the federal government most effectively acts as a "facilitator, convener, and source of information."²³ Since November 2010, a national task force led by DOJ and DHS has helped coordinate CVE-related community engagement from the national perspective. It works with U.S. Attorneys, DHS's Office for Civil Rights and Civil Liberties (CRCL), the Department of State, and DOJ, among others.²⁴

Role of U.S. Attorneys

Under the Administration's CVE strategy, U.S. Attorneys play a key role in community engagement within their jurisdictions.²⁵ U.S. Attorneys are "the nation's principal litigators under the direction of the Attorney General."²⁶ Attorney General Eric Holder has pushed the U.S. Attorneys to enhance their outreach efforts to Muslim, Sikh, and Arab American communities.²⁷ Within their districts across the country, U.S. Attorneys have met with Muslim communities regarding specific situations and trends.²⁸ In December 2010, DOJ began a pilot program involving U.S. Attorneys in community outreach efforts. This program did not specifically focus on CVE efforts but has included radicalization-related outreach.²⁹ For example, in September

²⁰ HSAC provides advice and recommendations to the Secretary of Homeland Security. The chair of the council is Judge William Webster, former Director of the CIA and Director of the FBI. Other members include leaders from state and local government, first responder communities, the private sector, and academia. The Countering Violent Extremism Working Group originated from a tasking by Secretary Napolitano to the HSAC in February 2010 to work with state and local law enforcement and relevant community groups to develop and provide recommendations on how DHS can better support community-based efforts to combat violent extremism domestically. See Homeland Security Advisory Council, Countering Violent Extremism Working Group, Spring 2010, p. 2. Hereinafter: HSAC CVE Working Group, Spring 2010.

²¹ HSAC CVE Working Group, Spring 2010, p. 5.

²² *Strategic Implementation Plan*, p. 10.

²³ *Empowering Local Partners*, p. 3.

²⁴ *Strategic Implementation Plan*, p. 9.

²⁵ *Ibid.*, p. 8.

²⁶ DOJ, "United States Attorneys' Mission Statement," <http://www.justice.gov/usao/about/mission.html>.

²⁷ DOJ, "Arab and Muslim Engagement: U.S. Attorneys' Outreach Efforts," http://www.justice.gov/usao/briefing_room/crt/engagement.html. Hereinafter: DOJ, "Arab and Muslim."

²⁸ DOJ, *Ten Years Later: The Justice Department After 9/11, Partnering with the Muslim, Arab, and Sikh Communities*, <http://www.justice.gov/911/partnerships.html>. Hereinafter: DOJ, *Ten Years Later*.

²⁹ *Strategic Implementation Plan*, p. 8.

2011, the U.S. Attorney for the District of Oregon and Attorney General Holder met with Arab and Muslim community representatives in Portland, OR.³⁰

Comparable outreach has been pursued by other U.S. Attorneys. The District of Minnesota has established the Young Somali-American Advisory Council. This responded to al-Shabaab's³¹ recruitment of young men within the greater Minneapolis-St. Paul, MN, Somali community.³² The council includes more than a dozen people between the ages of 18 and 30. Among the outreach activities tied to the council, the U.S. Attorney's office instructed council members on civics issues. In a similar vein, the U.S. Attorney for the Southern District of Florida and Assistant Attorney General Thomas E. Perez met with Muslim and Arab leaders in Miami in February 2011.³³ Likewise, in November 2010, an alleged jihadist terrorist plotter was arrested for purportedly attempting to bomb a Christmas tree lighting ceremony in Portland. In the plot's wake, the state's U.S. Attorney repeatedly met with local Muslim leaders.³⁴

Other Federal Activities

Currently, aside from the special role given to U.S. Attorneys, other elements of DOJ and additional U.S. government agencies engage and partner with Muslim American communities. Some of these efforts by DHS, DOJ, and FBI are detailed below.

Department of Homeland Security

DHS has stated that public outreach to local communities plays a major role in the department's mission.³⁵ Engagement activities are centered in the Office for Civil Rights and Civil Liberties (CRCL), which began its outreach in 2003.³⁶ Its work involves counterterrorism and CVE-related matters, but its overall mission is broader. The office is also responsible for³⁷

- advising DHS leadership, personnel, and partners about civil rights and civil liberties issues;

³⁰ DOJ, "Attorney General Holder Meets with Muslim Leaders in Portland," September 30, 2011, <http://blogs.usdoj.gov/blog/archives/1617?print=1>. Hereinafter: DOJ, "Attorney General Holder Meets."

³¹ A terrorist group in Somalia.

³² B. Todd Jones, U.S. Attorney for the District of Minnesota, "Arab and Muslim Engagement: Countering Violent Extremism through Community-Based Approaches," <http://www.justice.gov/usao/mn/opcd.html>; Laura Yuen, "Years After Somali Men Left Minn., Youth Decry Extremism," Minnesota Public Radio, November 8, 2011, <http://minnesota.publicradio.org/display/web/2011/11/08/young-minnesota-somalis-decry-extremism/>.

³³ DOJ, "Arab and Muslim."

³⁴ Peter Neumann, *Preventing Violent Radicalization in America*, Bipartisan Policy Center, (June 2011), p. 37 <http://www.bipartisanpolicy.org/sites/default/files/NSPG.pdf>. Hereinafter: Neumann, *Preventing Violent Radicalization*.

³⁵ CRCL, "Engagement with Key Communities Team," August 14, 2009. Hereinafter: CRCL, Engagement Team, August 14, 2009.

³⁶ CRCL, *Newsletter*, vol. 2, no. 1 (September 2011), http://www.aila.org/content/default.aspx?docid_36956. Hereinafter: CRCL, *Newsletter*, September 2011.

³⁷ The mission of the DHS Office for Civil Rights and Civil Liberties is outlined in 6 U.S.C. 345, http://www.dhs.gov/about/structure/editorial_0481.shtm. See DHS, Office of Civil Rights and Civil Liberties, <http://www.dhs.gov/about/structure/crcl.shtm>.

- communicating with individuals and communities whose civil rights and civil liberties may be affected by DHS activities, informing them about policies and avenues of redress, and promoting appropriate attention within DHS to their experiences and concerns; and
- investigating and resolving civil rights and civil liberties complaints filed by the public.

CRCL has a Community Engagement Section. Recent domestic CVE-related³⁸ outreach events have been coordinated by CRCL and its Community Engagement Section.³⁹

Department of Justice

In addition to the CVE role played by U.S. Attorneys, DOJ's engagement activities largely appear to come from the Civil Rights Division and the Community Relations Service.⁴⁰ According to its website, since the terrorist attacks of September 11, 2001 (9/11), the Civil Rights Division of DOJ has prioritized prosecution of bias crimes and discrimination against Muslims, Sikhs, and persons of Arab and South-Asian descent, as well as individuals perceived to be members of these groups. These types of incidents are commonly referred to as "backlash." The division has also educated people in these communities about their rights and available government services.⁴¹ Senior Civil Rights Division officials have met with Muslim, Sikh, Arab, and South Asian community leaders regarding backlash discrimination issues. Like the Civil Rights Division, DOJ's Community Relations Service is involved in outreach. Since 9/11, the service has held meetings around the country to address backlash-related issues.⁴²

Federal Bureau of Investigation

The FBI has publicly suggested that since 9/11, it has been formulating an "extensive program" to bolster its relationship with Arab, Muslim, Sikh, and South Asian communities in the United

³⁸ Much like CRCL, the Section's mission involves more than CVE. It reaches out to other communities whose issues are not necessarily tied to radicalization.

³⁹ CRCL, *Fiscal Year 2010 Annual and Consolidated Quarterly Reports to Congress*, September 20, 2011, pp. 14-15, <http://www.dhs.gov/xlibrary/assets/crcl-annual-report-fy-2010.pdf>; CRCL Engagement Team, August 14, 2009. DHS also provides law enforcement training related to CVE in the United States. With DOJ, DHS has instructed more than 46,000 "front line officers" on suspicious activity reporting. As of September 2011, CRCL taught over 2,000 law enforcement officials in the area of CVE. CRCL CVE training highlights topics such as understanding violent radicalization, cultural awareness, and community engagement. The training was developed "in response to concerns from attendees at community roundtables." See DIIS, Fact Sheet, "The Department of Homeland Security's Approach to Countering Violent Extremism," <http://www.dhs.gov/files/fact-sheet-approach-to-countering-violent-extremism.pdf> DIIS. Hereinafter: DIIS, Fact Sheet. See also: CRCL, *Newsletter*, vol. 1, no. 8 (June 2011), <http://www.aila.org/content/default.aspx?docid=36057>.

⁴⁰ DOJ, "Attorney General Holder Meets."

⁴¹ Civil Rights Division, "Initiative to Combat Post-9/11 Discriminatory Backlash," <http://www.justice.gov/crt/legalinfo/discrimupdate.php>. Hereinafter: Civil Rights Division, "Initiative."

⁴² *Ibid.*; Community Relations Service, *America's Peacemaker, Community Relations Service, U.S. Department of Justice, Annual Report, Fiscal Year 2010*, <http://www.justice.gov/crs/pubs/annualreport2010.pdf>; DOJ, *Ten Years Later*; Civil Rights Division, "Initiative." See Ondray T. Harris, Director, DOJ Community Relations Service, "Creating Positive Perception of Sikh Identity in the U.S. Public," speech at the 2nd Global Sikh Civil Rights Conference in Toronto, Canada, December 19, 2009, <http://www.justice.gov/crs/united-sikhs.pdf>.

States.⁴³ In March 2010, the chief of the Community Relations Unit of the FBI's Office of Public Affairs testified to Congress that the primary purpose of the agency's outreach program was "to enhance public trust and confidence in the FBI."⁴⁴ This involves fostering a positive image of law enforcement among U.S. organizations that have condemned terrorism and violent radicalization. The FBI relies on programs at the field office level to foster interaction with a wide variety of local groups.⁴⁵ Also, some FBI field offices have formally interacted with local Muslim communities regarding specific cases.⁴⁶ At the national level, FBI headquarters representatives have engaged in liaison with Arab and Muslim American advocacy groups and have regular issue-focused conference calls with community leaders.⁴⁷ The FBI is also a member of the Incident Coordination Communications Team managed by DHS CRCL.

Risks and Challenges

Although there is considerable support among public officials for community engagement, some experts warn of significant challenges in the development of programs that foster substantive relationships rather than token discussions or community relations events. A study of policing in Arab American communities sponsored by the National Institute of Justice, for example, highlighted four key obstacles hindering outreach between U.S. Arabs (Christian and Muslim) and law enforcement: "Distrust between Arab communities and law enforcement, lack of cultural awareness among law enforcement officers, language barriers, and concerns about immigration status and fears of deportation."⁴⁸

Terrorism expert Marc Sageman cautions that engagement can be a sign of government focus on Muslim communities when instead it should be stressed that Muslims are Americans just like everyone else.⁴⁹ He sees another challenge arise when engagement on the government side is led by federal agencies with law enforcement and intelligence responsibilities. "It can send the message that we are only interested in Muslims because they are potential law breakers. No other foreign or religious communities in the United States get this type of scrutiny."⁵⁰

⁴³ Scott Atran, *Senate Armed Services Subcommittee on Emerging Threats and Capabilities: Countering Violent Extremism: Statement for the Record, Addendum-2*, 111th Cong., 2nd sess., March 10, 2010, <http://armed-services.senate.gov/statemnt/2010/03%20March/Atran%2003-10-10.pdf>. Hereinafter: Atran Testimony, March 10, 2010.

⁴⁴ Brett Hovington, *House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment: Working with Communities to Disrupt Terror Plots: Statement for the Record*, 111th Cong., 2nd sess., March 17, 2010, <http://homeland.house.gov/SiteDocuments/20100317103507-03554.pdf>. Hereinafter: Hovington Testimony, March 17, 2010.

⁴⁵ Hovington Testimony, March 17, 2010. See also: FBI, "Building Trust: The Arab, Muslim, and Sikh Advisory Council," June 1, 2009, <http://washingtondc.fbi.gov/trust060109.htm>.

⁴⁶ Hovington Testimony, March 17, 2010.

⁴⁷ Atran Testimony, March 10, 2010.

⁴⁸ Nicole J. Henderson et al., *Policing in Arab-American Communities After September 11*, National Institute of Justice, Washington, DC, July 2008, p. ii. For the full study, see Nicole J. Henderson et al., *Law Enforcement and Arab American Community Relations After September 11, 2001: Engagement in a Time of Uncertainty*, Vera Institute of Justice, New York, NY, June 2006, <http://www.vera.org/policerelations>. As its title clearly suggests, this project examined the experiences of Arab-Americans, two thirds of whom are Christian.

⁴⁹ Discussion with CRS, April 7, 2010. Sageman is an independent researcher on terrorism, founder of Sageman Consulting, LLC, and author of *Leaderless Jihad: Terror Networks in the Twenty-First Century* (University of Pennsylvania Press, 2008).

⁵⁰ *Ibid.*

Outreach may be most effective when U.S. Muslim communities initiate it and community-government contact revolves around countering the extremist messages popular among violent jihadists.⁵¹ Marc Sageman also suggests it would be more appropriate for local authorities, such as a mayor's office, to perform the engagement role because they know these communities better than federal officials.

The Tension Between Enforcement and Engagement Activities

An inherent challenge to building trust and partnership involves law enforcement investigative activities and tactics that can be perceived to unfairly target law-abiding citizens or infringe on speech, religion, assembly, or due process rights. This challenge highlights how government counterterrorism work in the secretive operational realm depicted in **Figure 1** can influence engagement conducted in the open marketplace of ideas. If a community views government counterterrorism investigative activity as overly aggressive, it may not willingly cooperate in engagement programs. One expert has noted that "counter-radicalization is not about intelligence-gathering nor is it primarily about policing."⁵² The HSAC Countering Violent Extremism Working Group found that

There can be tension between those involved in law enforcement investigations and those collaborating to establish local partnerships to stop violent crime. Community policing can be impeded if other enforcement tactics are perceived as conflicting with community partnership efforts.⁵³

This challenge is evident in some public discussions of law enforcement surveillance activities and efforts to recruit and manage informants. Revelations that the NYPD engaged in surveillance of mosques, Muslim businesses, and Muslim college students in New Jersey and elsewhere in 2006 and 2007 have prompted concern among a number of community groups and civil libertarians.⁵⁴ The FBI's top official in New Jersey suggested that such activities undermined the bureau's efforts at community engagement.⁵⁵ While New York City Mayor Michael Bloomberg and others defended the legality of such activities, some New Jersey officials have complained that the NYPD had not effectively coordinated efforts with them.⁵⁶ Other former law enforcement officials in New Jersey believed that appropriate cooperation occurred.⁵⁷ Also, as announced in May 2012, a fact-finding review conducted by New Jersey's Office of the Attorney General "revealed no evidence ... that NYPD's activities in the state violated New Jersey civil or criminal laws."⁵⁸

⁵¹ Gartenstein-Ross and Grossman, *Homegrown Terrorists in the U.S. and U.K.*, p. 60.

⁵² Neumann, *Preventing Violent Radicalization.*, p. 19.

⁵³ HSAC CVE Working Group, Spring 2010, p 6.

⁵⁴ Samantha Henry. "NJ Muslims, Officials Discuss NYPD Surveillance," *Associated Press*, March 3, 2012. Hereinafter: Henry "NJ Muslims, Officials." Chris Hawley, "NYPD Monitored Muslim Students All Over Northeast," *Associated Press*, February 18, 2012.

⁵⁵ Samantha Henry. "NJ FBI Says NYPD Monitoring Damaged Muslims' Trust," *Associated Press*, March 8, 2012.

⁵⁶ Henry, "NJ Muslims, Officials;" Jason Grant, "Recent NYPD Spying Uproar Shakes FBI's Foundations in N.J. Terror Intelligence," *Star-Ledger*, March 7, 2012, http://www.nj.com/news/index.ssf/2012/03/recent_nypd_spying_uproar_shak.html.

⁵⁷ Christopher Baxter. "Secret NYPD Surveillance in N.J. Was Not So Secret. Former Officials Say," *Star-Ledger*, March 6, 2012, http://www.nj.com/news/index.ssf/2012/03/secret_nypd_surveillance_in_nj.html.

⁵⁸ New Jersey Office of the Attorney General, press release, "Office of the Attorney General Takes Steps to Address (continued...)"

In pursuing a community engagement strategy, the use of informants can be a controversial issue, especially when law enforcement officials rely on informants with criminal records who may be working on behalf of authorities in exchange for reduced jail time. One Muslim community leader who has published widely on domestic terrorism states that “many Muslim Americans fear that paid FBI informants specifically target impressionable youth and that law enforcement agents coerce community members to become informants themselves to avoid complications with immigration procedures.”⁵⁹ Confidential informants have been used in post-9/11 violent jihadist cases occurring in the United States. In some of those cases, the informants had criminal histories. The use of informants poses the following risks:

Informants do not merely observe and collect data. They make things happen.... Informants can cause confusion and dissatisfaction among members of groups and communities they infiltrate, discrediting leaders, and fostering factionalism as people wonder if any of their colleagues are spies. Their handlers’ structure of incentives—raises, promotions, transfers, financial rewards, waived jail time—creates a system where informants consciously or subconsciously create and then destroy terrorist threats that would not otherwise exist. These pressures can push them from passive observer to aggressive actor, with serious consequences for constitutionally protected free speech. Another unplanned result: government loses legitimacy and support in the eyes of targeted communities, if they feel they have been manipulated.⁶⁰

Acknowledging the challenge, FBI Director Robert Mueller said in 2009, “Oftentimes, the communities from which we need the most help are those who trust us the least. But it is in these communities that we ... must redouble our efforts.”⁶¹ Also in 2009, then-FBI spokesman John

(...continued)

Out-of-State Law Enforcement Activity in New Jersey Following Fact-Finding Review,” May 24, 2012, <http://www.nj.gov/oag/newsreleases12/pr20120524b.html>.

⁵⁹ Alejandro J. Beutel, “Muslim Americans and U.S. Law Enforcement: Not Enemies, But Vital Partners,” *The Christian Science Monitor*, December 30, 2009, <http://www.csmonitor.com/Commentary/Opinion/2009/1230/Muslim-Americans-and-US-law-enforcement-not-enemies-but-vital-partners>. For more information on controversies surrounding informants, see Peter Finn, “Documents Provide Rare Insight Into FBI’s Terrorism Stings,” *Washington Post*, April 13, 2012, http://www.washingtonpost.com/world/national-security/documents-provide-rare-insight-into-fbis-terrorism-stings/2012/04/13/gIQA5J6CGI_story.html; Jerry Markon, “Lawsuit Alleges FBI Violated Muslims’ Freedom of Religion,” *Washington Post*, February 22, 2011, <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/22/AR2011022206975.html>; Jerry Markon, “Mosque Infiltration Feeds Muslims’ Distrust of FBI,” *Washington Post*, December 5, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/04/AR2010120403720.html>; Salvador Hernandez, “Release Terms Eased for Man Accused of Lying About Alleged Terrorist Ties,” *The Orange County Register*, June 11, 2010, <http://www.ocregister.com/articles/niazi-252994-fbi-case.html?pic=1>; Trevor Aronson, “FBI Tries to Deport Muslim Man for Refusing to be an Informant,” *miaminewtimes.com*, Oct 8, 2009, <http://www.miaminewtimes.com/2009-10-08/news/unholy-war-fbi-tries-to-deport-north-miami-beach-imam-foad-farahi-for-refusing-to-be-an-informant/>; “FBI Creates Climate of Fear,” *Orange County Register*, Editorial, March 22, 2009, <http://www.ocregister.com/articles/fbi-18893-ocprint-fear-.html>; Teresa Watanabe and Paloma Esquivel, “L.A. Area Muslims Say FBI Surveillance Has a Chilling Effect on Their Free Speech and Religious Practices,” *Los Angeles Times*, March 1, 2009, <http://articles.latimes.com/2009/mar/01/local/me-muslim1>. Hereinafter: Watanabe and Esquivel, March 1, 2009. Thomas Cincotta, “From Movements to Mosques, Informants Endanger Democracy,” *The Public Eye*, summer 2009, <http://www.publiceye.org/magazine/v24n2/movements-to-mosques.html>. Hereinafter: Cincotta, “From Movements to Mosques.” Lee Romney, “Immigrant Says FBI Tried Threats to Make Him Spy,” *Los Angeles Times*, August 12, 2006; <http://www.chron.com/disp/story.mpl/front/4112103.html>. Peter Waldman, “A Muslim’s Choice: Turn U.S. Informant or Risk Losing Visa,” *Wall Street Journal*, July 11, 2006, <http://www.legalsanctuary.org/doc/article13970.pdf>.

⁶⁰ Cincotta, “From Movements to Mosques.”

⁶¹ Quoted in Mathai Kuruvila, “U.S. Muslims Debate How Much to Help FBI,” *San Francisco Chronicle*, April 6, 2009, [http://articles.sfgate.com/2009-04-06/news/17193854_1_american-muslim-taskforce-muslim-community-\(continued...\)](http://articles.sfgate.com/2009-04-06/news/17193854_1_american-muslim-taskforce-muslim-community-(continued...))

Miller said the agency values its relationships with Muslims and has worked hard on outreach efforts that range from town hall meetings to diversity training for FBI agents.⁶² Miller said there is no factual basis for claims the FBI infiltrates mosques or conducts blanket surveillance of Muslim leaders. “Based on information of a threat of violence or a crime, we investigate individuals, and those investigations may take us to the places those individuals go.”⁶³

Former FBI agents and federal prosecutors note that informants are “still one of the government’s best weapons to thwart terrorists and that the benefit to national security is likely to far outweigh any embarrassment to the agency.” They claim that “although the law places almost no constraints on the use of informants, the agency takes sending an informant into a mosque very seriously and imposes a higher threshold for such requests.”⁶⁴ Former FBI counterterrorism Chief Robert Blitzer states that “what matters to the FBI is preventing a massive attack that might be planned by some people ... using the mosque or church as a shield because they believe they’re safe there. That is what the American people want the FBI to do. They don’t want some type of attack happening on U.S. soil because the FBI didn’t act on information.”⁶⁵

Maher Hathout from the Muslim Public Affairs Council counters by saying that “people cannot be suspects and partners at the same time. Unless the FBI’s style changes, the partnership with the Muslim community will not be fruitful.”⁶⁶ The HSAC’s CVE Working Group also cautions that “Law enforcement should be sensitive to the fact that perceptions regarding enforcement actions and intelligence gathering can impact community-oriented policing goals.”⁶⁷ In considering the tradeoff between security and liberty, policy makers face a choice in those cases where an investigative tactic might inflame members of a particular community: Is the impact of that tactic counterproductive in the long run, or is it necessary, short-term collateral damage?

U.S. Attorneys as Brokers

As mentioned elsewhere in this report, DOJ has pushed the U.S. Attorneys to become larger players in community outreach. This suggests a critical question: is it appropriate to have the nation’s principal litigators be key players in the federal government’s CVE outreach efforts? Can the same people responsible for prosecuting terrorism cases effectively broker trust among community members who may be wary of federal law enforcement? Maintaining the integrity of

(...continued)

american-islamic-relations.

⁶² Quoted in Samantha Henry, “Some Muslims Rethink Close Ties to Law Enforcement,” *Associated Press*, May 4, 2009, http://www.breitbart.com/article.php?id=D97VH09O0&show_article=1.

⁶³ *Ibid.* In March 2012, the American Civil Liberties Union (ACLU) asserted that the FBI had used outreach efforts at mosques in California to gather intelligence. Much of the outreach activity critiqued by the ACLU occurred several years ago. FBI denied that the outreach was used to gather intelligence. See http://www.aclu.org/files/assets/aclu_eye_on_the_fbi_-_mosque_outreach_03272012_0.pdf; Dan Levine, “FBI Said to Have Gathered Intelligence on California Muslims,” *Reuters*, March 27, 2012, <http://www.reuters.com/article/2012/03/28/us-usa-california-muslims-idUSBRE82R00Y20120328>.

⁶⁴ Gillian Flaccus, “Calif. Case Highlights Use of Mosque Informants,” *Associated Press*, March 1 2009, http://www.breitbart.com/article.php?id=D96LD2A81&show_article=1.

⁶⁵ *Ibid.*

⁶⁶ Watanabe and Esquivel, March 1, 2009.

⁶⁷ HSAC CVE Working Group, Spring 2010, p. 6.

this dualistic U.S. Attorney role—chief terrorism litigators v. federal outreach coordinators—may be challenging in the implementation of the strategy.

Legitimacy and Litmus Tests

Given their role in federal CVE engagement, U.S. Attorneys have to selectively cooperate with groups at the local level. Identifying specific groups for outreach may be challenging. There is little consensus among American Muslims regarding national advocacy groups: “many Muslims do not feel there is a national Muslim-American organization that represents them. When asked which of a list of national Muslim-American organizations represents their interests, 55% of Muslim men and 42% of Muslim women say that none do.”⁶⁸

The U.S. government can affect the legitimacy of community actors simply by choosing them as outreach partners. It is unclear how U.S. Attorneys will select the groups with which they will work. To this end, will the U.S. government establish litmus tests regarding federal interaction with community groups? What role will law enforcement considerations—potentially choosing only groups that have cooperated with FBI investigations by offering leads or providing informants, for example—play in the selection of community partners? Will federal investigators scour the backgrounds of groups prior to engaging with them?

When selecting engagement partners, DOJ has made at least one very public choice that was driven by law enforcement or prosecutorial considerations. The FBI and DOJ have limited their ties to the Council on American-Islamic Relations (CAIR), because DOJ listed the group as an unindicted co-conspirator in a federal terrorism case.⁶⁹ This is an example of the dynamics described in **Figure 1**—the secretive (operational) realm driving community engagement activity in the marketplace of ideas. In November 2008, the Holy Land Foundation for Relief and Development and five of its leaders were convicted of providing material support to Hamas, a designated foreign terrorist organization.⁷⁰ CAIR has opposed its listing as an unindicted co-conspirator. The listing is not a formal criminal charge, and subsequent terrorism charges have not been brought against CAIR.⁷¹ In spite of all of this, CAIR, a well-known Muslim advocacy group, maintains working relationships with local law enforcement officials.⁷²

⁶⁸ *Muslim Americans: Faith, Freedom, and the Future; Examining U.S. Muslims' Political, Social, and Spiritual Engagement 10 Years After September 11*, Abu Dhabi Gallup Center, August 2011, p. 25, <http://www.abudhabigallupcenter.com/148778/REPORT-BILINGUAL-Muslim-Americans-Faith-Freedom-Future.aspx>. Hereinafter: *Muslim Americans: Faith, Freedom, and the Future*.

⁶⁹ Letter from Richard C. Powers, FBI Assistant Director, to U.S. Senator Jon Kyl, April 28, 2009.

⁷⁰ Transcript of Hearing, “Rep. Frank R. Wolf Holds a Hearing on Justice Department Budget,” *Political Transcript Wire*, March 1, 2012; DOJ, press release, “Federal Judge Hands Downs Sentences in Holy Land Foundation Case,” May 27, 2009, <http://www.justice.gov/opa/pr/2009/May/09-nsd-519.html>. For more on CAIR’s origins and relationship with the U.S. government, see Lorenzo Vidino, *The New Muslim Brotherhood in the West* (New York: Columbia University Press, 2010), pp. 177-197. In the fall of 2008, the FBI limited its interactions with CAIR.

⁷¹ CAIR, press release, “Top Internet Disinformation About CAIR,” http://www.cair.com/Portals/0/pdf/Dispelling_Rumors_about_CAIR.pdf.

⁷² Scott Shane, “Congressional Hearing Puts Muslim Civil Rights Group in the Hot Seat Again,” *New York Times*, March 11, 2011, <http://www.nytimes.com/2011/03/12/us/politics/12muslims.html?scp=3&sq=&st=nyt>.

Fusion Centers and Community Engagement—Potentially Alleviating Tensions

The CVE strategy mentions the role of the national network of fusion centers⁷³ in alleviating tension between the government’s investigative and engagement activities. Fusion centers play a part in reporting suspicious, terrorism-related activity nationwide, perhaps potentially causing some tension between communities and law enforcement.⁷⁴ The strategy and the SIP mention the Building Communities of Trust Initiative (BCOT) as a project fostering relationships among three sets of actors—fusion centers, law enforcement, and the communities in which they operate.⁷⁵ This type of outreach potentially informs local communities about how suspicious activity suggestive of terrorism is reported to law enforcement and how police protect civil rights and liberties as they look for such activity.⁷⁶ The initiative’s recommendations included items such as

- training of fusion center analysts in cultural sensitivity so that they can distinguish behavior that is constitutionally protected from criminal or terrorist activity;
- encouraging law enforcement to “embrace” community policing by “emphasizing partnerships and problem solving”; and
- encouraging communities to view information sharing with fusion centers and law enforcement as key to crime prevention and counterterrorism.⁷⁷

Building Government and Law Enforcement Expertise

The SIP emphasizes three key items in this area. First, the plan notes that the U.S. government has to improve its understanding of radicalization via research, analysis, and partnerships. Second, greater sharing of information among state, local, and federal agencies regarding terrorist recruitment and radicalization is necessary.⁷⁸ Third, the SIP notes that the federal government has to improve the radicalization-related training offered to federal, state, and local agencies.

Paramount among the federal government’s efforts to improve its understanding of CVE are efforts to study the radicalization process and identify radicalizing individuals. To this end, as of March 2012, the National Institute of Justice included research on domestic radicalization in its preliminary list of forthcoming funding opportunities.⁷⁹ The Science and Technology Directorate (S&T) within DHS has also pursued the topic. The department claims that since 2009, S&T has

⁷³ DHS recognizes a national network of state and local intelligence fusion centers. The network consists of centers that function as “collaborative effort[s] of two or more agencies that provide resources, expertise, and information ... with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.” See *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, August 2006, p. 12. http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf. For a list of fusion centers, see Department of Homeland Security, “Fusion Center Locations and Contact Information,” February 22, 2012, http://www.dhs.gov/files/programs/gc_1301685827335.shtm.

⁷⁴ For more on suspicious activity reporting see CRS Report R40901, *Terrorism Information Sharing and the Nationwide Suspicious Activity Reporting Initiative: Background and Issues for Congress*, by Jerome P. Bjelopera.

⁷⁵ See Robert Wasserman, *Guidance for Building Communities of Trust*, July 2010, pp. 4-5, http://nsi.ncirc.gov/documents/e071021293_BuildingCommTrust_v2-August%2016.pdf. Hereinafter: Wasserman, *Guidance for Building*.

⁷⁶ *Strategic Implementation Plan*, p. 9.

⁷⁷ Wasserman, *Guidance for Building*, pp. 4-5.

⁷⁸ *Strategic Implementation Plan*, pp. 12-18.

⁷⁹ See <http://www.nij.gov/nij/funding/forthcoming.htm>. For the Congressional appropriation see P.L. 112-55, p. 615.

developed more than 20 reports in this area.⁸⁰ To help identify radicalizing individuals, DHS, the FBI, and the National Counterterrorism Center (NCTC) produced a study of homegrown terrorists, which reportedly teased out warning signs of radicalization. The study was discussed by senior federal, state, and local law enforcement officials at the White House in January 2012.⁸¹ Along these same lines, in July 2011, NCTC released findings resulting from an interagency study of homegrown terrorists. This study was not made public officially, but a summary of its findings is available online. It describes four “mobilizing patterns” among extremists. These include “links to known extremists, ideological commitment to extremism, international travel, and pursuit of weapons and associated training.”⁸² It also emphasized an approach to understanding and assessing radicalization via analysis of behavioral indicators.⁸³

The SIP also calls for enhanced information sharing between federal, state, and local law enforcement. Prior to late 2011, these efforts largely revolved around disseminating information to and briefing state and local officials. Such activity included the development of case studies examining the experiences of known and suspected terrorists.⁸⁴ This was recommended in 2010 by the HSAC.⁸⁵ In February 2011 congressional testimony, DHS Secretary Janet Napolitano remarked that DHS develops these *unclassified* case studies so

that state and local law enforcement, state and local governments, and community members can understand the warning signs that could indicate a developing terrorist attack. These case studies focus on common behaviors and indicators regarding violent extremism to increase overall situational awareness and provide law enforcement with information on tactics, techniques, and plans of international and domestic terrorists.⁸⁶

Napolitano went on to note that DHS conducted what she dubbed “deep dive sessions” regarding CVE issues with local police intelligence experts—providing them with information they could pass to subordinates.⁸⁷

Additionally, the SIP notes that the federal government will enhance the radicalization-related training offered to federal, state, and local agencies. It argues that this is necessary because of “a small number of instances of federally sponsored or funded CVE-related and counterterrorism training that used offensive and inaccurate information.”⁸⁸ In March 2011, news reports and a study suggested that state and local law enforcement officials were receiving poor counterterrorism training from unqualified instructors, often from the private sector.⁸⁹

⁸⁰ DHS, Fact Sheet, p. 2.

⁸¹ Eileen Sullivan, “Police Chiefs Meet at WH on Homegrown Terror Fight,” *Associated Press*, January 18, 2012.

⁸² National Counterterrorism Center. “Behavioral Indicators Offer Insights for Spotting Extremists Mobilizing for Violence, July 22, 2011, p. 1.

⁸³ *Ibid.*

⁸⁴ *Strategic Implementation Plan*, p. 14.

⁸⁵ HSAC CVE Working Group. Spring 2010, p. 20.

⁸⁶ U.S. Congress, House of Representatives Committee on Homeland Security, Written Testimony of Janet Napolitano, Secretary of the Department of Homeland Security, “Understanding the Homeland Threat Landscape—Considerations for the 112th Congress,” 112th Cong., 1st sess., February 9, 2011, p. 5.

⁸⁷ *Ibid.*

⁸⁸ *Strategic Implementation Plan*, p. 15.

⁸⁹ Dina Temple-Raston, “New Concern About Bias In Counterterror Training,” *National Public Radio*, March 9, 2011, http://www.npr.org/2011/03/09/134374232/new-concern-about-bias-in-counterterror-training?ps_rs; Thomas Cincotta, *Manufacturing the Muslim Menace: Private Firms, Public Servants, and the Threat to Rights and Security*, 2011, (continued...)

Furthermore, news reports indicated that offensive material produced by an FBI employee was delivered in a variety of official training sessions up until August 2011.⁹⁰ These revelations led to concerns from public officials and advocacy groups regarding training standards used by the bureau.⁹¹ In addition, reportedly biased material had seeped into the training made available to Joint Terrorism Task Force⁹² officers via a secure computer network.⁹³

In the midst of these revelations, in September 2011 the bureau announced a review

of all training and reference materials that relate in any way to religion or culture. Additionally, the FBI will consult with outside experts on the development and use of training materials to best ensure the highest level of quality for new agent training, continuing education for all employees, and any FBI-affiliated training. All training will be consistent with FBI core values, the highest professional standards, and adherence to the Constitution.⁹⁴

DOJ announced a similar review in September 2011 as well.⁹⁵ Less than one percent of the material inspected was found to be inaccurate or inappropriate.⁹⁶ In October 2011, the White House ordered a broader examination of CVE instructional efforts within the federal government.⁹⁷ In the same month, DHS released guidance and best practices for CVE training. These highlighted five commonsense goals:

(...continued)

Public Research Associates. http://www.publiceye.org/liberty/training/Muslim_Menace_Complete.pdf.

⁹⁰ Spencer Ackerman and Noah Shachtman, "Video: FBI Trainer Says Forget 'Irrelevant' al-Qaida, Target Islam," *Wired*, September 20, 2011, <http://www.wired.com/dangerroom/2011/09/fbi-islam-qaida-irrelevant/all/1>.

⁹¹ Letter from Sen. Joseph I. Lieberman and Sen. Susan M. Collins, to Eric H. Holder, Jr., Attorney General, and Janet Napolitano, Secretary of Homeland Security, March 29, 2011. <http://www.hsgac.senate.gov/reports/letters>. For an example of concerns voiced by advocacy groups see Letter from American Civil Liberties Union et al., to Robert S. Mueller, III, Director, Federal Bureau of Investigation, October 4, 2011, http://www.aclu.org/files/assets/sign_on_letter_to_dir_mueller_re_radicalization_report_10.4.11.pdf. Some Members of Congress also wrote to Attorney General Eric H. Holder, Jr. and Secretary of Defense Leon E. Panetta regarding potential censorship of training material after the fallout surrounding the FBI's training efforts. See Letter from Rep. Sue Myrick et al. to Eric H. Holder, Jr., Attorney General, and Leon E. Panetta, Secretary of Defense, December 15, 2011, http://myrick.house.gov/uploads/12152011_Letter%20to%20DOJ%20and%20DOD%20re%20CT%20training%20changes.pdf.

⁹² Joint Terrorism Task Forces (JTTFs) are locally based, multi-agency teams of investigators, analysts, linguists, SWAT experts, and other specialists who investigate terrorism and terrorism-related crimes. Seventy-one of the more than 100 JTTFs currently operated by DOJ and the FBI were created since 9/11. Over 4,400 federal, state, and local law enforcement officers and agents—more than four times the pre-9/11 total—work in them. These officers and agents come from more than 600 state and local agencies and 50 federal agencies. See Federal Bureau of Investigation, "Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces," http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jtfts.

⁹³ Spencer Ackerman, "Obama Orders Government to Clean Up Terror Training," *Wired*, November 29, 2011, <http://www.wired.com/dangerroom/2011/11/obama-islamophobia-review/>. Hereinafter: Ackerman, "Obama Orders."

⁹⁴ FBI, press release, "FBI Launches Comprehensive Review of Training Program," September 20, 2011, <http://www.fbi.gov/news/pressrel/press-releases/fbi-launches-comprehensive-review-of-training-program>.

⁹⁵ James M. Cole, Deputy Attorney General, memorandum for heads of DOJ components and United States Attorneys, "Training Guiding Principles," March 20, 2012, <http://www.justice.gov/dag/training-guiding-principles.pdf>. Hereinafter, Cole, memorandum.

⁹⁶ Letter from Greg Fowler, Special Agent in Charge, FBI Portland Division, to Community Partners, March 28, 2012, http://www.fbi.gov/portland/news-and-outreach/stories/letter-to-community-partners?utm_campaign_email-Immediate&utm_medium=email&utm_source=portland-top-stories&utm_content=83167.

⁹⁷ Ackerman, "Obama Orders."

1. Trainers and training should be expert and well-regarded.
2. Training should be sensitive to constitutional values.
3. Training should facilitate further dialog and learning.
4. Training should adhere to government standards and efforts.
5. Training and objectives should be appropriately tailored, focused, and supported.⁹⁸

The same document notes that CVE education programs differ from strictly counterterrorism training (the latter presumably centered on topics such as terrorist threats, vulnerabilities, and trends in terrorism). CVE training focuses “on developing trust, enhancing community resiliency, prevention, intervention, and protecting civil rights and civil liberties.”⁹⁹ In March 2012, DOJ and FBI released their own sets of training principles that parallel DHS’s goals.¹⁰⁰

Risks and Challenges

Development of better training and improved information sharing are laudable law enforcement goals. However, because such efforts feature so prominently in the second SIP objective, its overall thrust may be perceived to be more about classic preventative policing than about countering radicalization at the grass-roots level. It is unclear how much of the activity described under this objective directly fits into the Administration’s emphasis on “a community based” CVE approach.¹⁰¹

There is space in the CVE strategy for training law enforcement about constitutionally protected aspects of the radicalization process—in other words, efforts to train police to understand when suspects go from being law-abiding radicals to being terrorists. However, the SIP itself does not offer any formal means for federal, state, or local law enforcement to cope with radicalizing individuals outside of their traditional areas of expertise—investigation, arrest, and prosecution. The SIP does not outline mechanisms for law enforcement to refer radicalizing individuals for community intervention (whatever that might mean within a local context). Without such a process, police can become very adept at identifying radicalization and yet be only able to cope with a radicalized individual when he or she mobilizes and becomes a terrorism suspect. One of the risks implicit in this SIP objective is that it may sharpen police ability to investigate terrorists, without improving their ability to intervene with radicalizing individuals.

⁹⁸ CRCL, *Countering Violent Extremism (CVE) Training Guidance and Best Practices*, 2011, <http://training.fema.gov/EMIWeb/docs/shared/CVE.%20Training%20Guidance.pdf>. Hereinafter: CRCL, *Training Guidance*. The Federal Emergency Management Agency (FEMA) also issued a bulletin regarding the same issues. FEMA grants can be used for CVE training. See FEMA, *Grant Programs Directorate Information Bulletin*, October 7, 2011, <http://www.fema.gov/pdf/government/grant/bulletins/info373.pdf>.

⁹⁹ CRCL, *Training Guidance*. DHS defines “resiliency” as the “ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions.” See; HSAC, *Community Resilience Task Force Recommendations*, June 2011, p. 8, <http://www.dhs.gov/xlibrary/assets/hsac-community-resilience-task-force-recommendations-072011.pdf>.

¹⁰⁰ Cole, memorandum; FBI, *The FBI’s Guiding Principles: Touchstone Document on Training 2012*, March 2012, <http://www.fbi.gov/about-us/training/the-fbis-guiding-principles>.

¹⁰¹ *Empowering Local Partners*, p. 2.

If the SIP's efforts to improve law enforcement training mostly enhance the ability of police to detain suspects and provide no other means for coping with radicalization, then these elements of the strategy might be better described as counterterrorism in nature, not part of the nation's counter-radicalization strategy.

The Issue of Openness

Should the federal government be concerned about the over-classification of radicalization-related research and training material by the security agencies involved in its development? The SIP's second objective is an area in which a great deal of activity can occur behind closed doors (within the secretive realm described in **Figure 1**), especially if the objective largely involves security, intelligence, and law enforcement agencies that typically avoid public disclosure of much of their other work. *However*, the steps involved in the radicalization process involve largely constitutionally protected activity that occurs in the public sphere. Excessive secretiveness regarding government efforts to understand the legally protected activities of Americans might actually fuel radicalization. For example, one study by a British think tank has suggested that conspiracy theories “are a reaction to the lack of transparency and openness in many of our [U.K.] institutions.” This same study sees conspiracies as a “radicalizing multiplier.”¹⁰² Could this be possible in the United States?

A project developed as part of the second SIP objective was not widely released. The study of radicalization among homegrown violent extremists performed by DHS, NCTC, and the FBI—mentioned above—was revealed to state and local law enforcement behind closed doors at the White House. This example poses the question: can the federal government build trust within local communities if it holds back from the general public its own study of how people in the United States radicalized and became terrorists? Will secretiveness in this area actually feed radical narratives?

Additionally, will excessively secret government efforts to understand radicalization shake community trust in law enforcement? Federal attempts to develop *classified* theories about legally protected activities may make community groups less willing to “share” information regarding those very activities—*especially if that information is treated strictly as intelligence by the government and the results of such “sharing” are never seen*. Transparency in this arena potentially opens government conceptualizations of radicalization and federal training materials to the scrutiny of outside experts. It is unclear what sway partnerships with non-government experts will have in the SIP's second objective.

Talking about Ideology

Ideology is a key ingredient in the radicalization experience. It is unclear how the CVE Training Guidance issued by DHS accommodates discussion of ideology within an instructional environment. In fact, under one of its goals: “Training should be sensitive to constitutional values,” the guidance indicates that “Training should focus on behavior, not appearance or membership in particular ethnic or religious communities,” yet it is silent regarding radical

¹⁰² Jamie Bartlett and Carl Miller, *The Power of Unreason: Conspiracy Theories, Extremism, and Counter-Terrorism*, Demos, London, August 29, 2010, pp. 21, 39.

ideologies. Should instructors focus on ideology? How should instructors discuss radical beliefs in the classroom?

Countering Violent Extremist Propaganda

The SIP notes that countering violent extremist propaganda is “the most challenging area of work, requiring careful consideration of a number of legal issues, especially those related to the First Amendment.”¹⁰³ In this area the document highlights NCTC’s efforts to develop a “Community Awareness Briefing.” In 2010, NCTC’s Director described the briefing in testimony to the Senate Homeland Security and Governmental Affairs Committee:

It has become clear that government can play a significant role by acting as a convener and facilitator that informs and supports—but does not direct—community-led initiatives. Based on this, NCTC led the development of a Community Awareness Briefing that conveys unclassified information about the realities of terrorist recruitment in the Homeland and on the Internet. The briefing, which can be used by departments and agencies and has garnered very positive reactions, aims to educate and empower parents and community leaders to combat violent extremist narratives and recruitment.¹⁰⁴

NCTC has also connected community activists with technology experts in a seminar to “maximize the use of technology to counter violent extremism online” and the Department of State has developed exchanges between foreign CVE experts and U.S. communities.¹⁰⁵ The SIP did not indicate any additional “current activity” in late 2011 to counter violent extremist propaganda other than working to inform the media, policy makers, and U.S. communities on the issue. It does mention the development of a separate strategy for the digital environment.¹⁰⁶

Risks and Challenges

The SIP notes that government efforts to counter narratives that foster radicalization should affirm American unity and bolster community capacities to “contest violent extremist ideas.” The document stresses the importance of First Amendment concerns in this area.¹⁰⁷

Aside from First Amendment issues, a challenge in this area might revolve around the perceived legitimacy of the main agencies the Administration selects for its implementation efforts. If security agencies trawling the Internet for potential suspects lead the charge in fostering a counter-narrative, will American Muslims see these efforts as legitimate?¹⁰⁸ How willing will they be to partner with FBI, DOJ, NCTC, and DHS to further this SIP goal?

¹⁰³ Ibid., p. 18.

¹⁰⁴ Written Statement of Michael Leiter; Director, National Counterterrorism Center; U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland*, 111th Cong., 2nd sess., September 22, 2010, p. 8.

¹⁰⁵ *Strategic Implementation Plan*, p. 19.

¹⁰⁶ Ibid., p. 20.

¹⁰⁷ Ibid., p. 18.

¹⁰⁸ See CRS Report R42406, *Congressional Oversight of Agency Public Communications: Implications of Agency New Media Use*, by Kevin R. Kosar, for information regarding Congress’s role in oversight of federal public communications activities.

One area in which these agencies may be able to leverage their reputations as part of the U.S. counterterrorism apparatus, build rapport within communities, and possibly forward efforts to counter extremist propaganda, involves personal online security. They can provide training regarding safe Internet navigation, how to avoid criminals online, and websites sponsored by officially listed foreign terrorist organizations. They can talk to communities about what types of online activities prosecuted terrorists pursued, especially those activities documented in court proceedings and government press releases.

Administration Plan and Future Activities

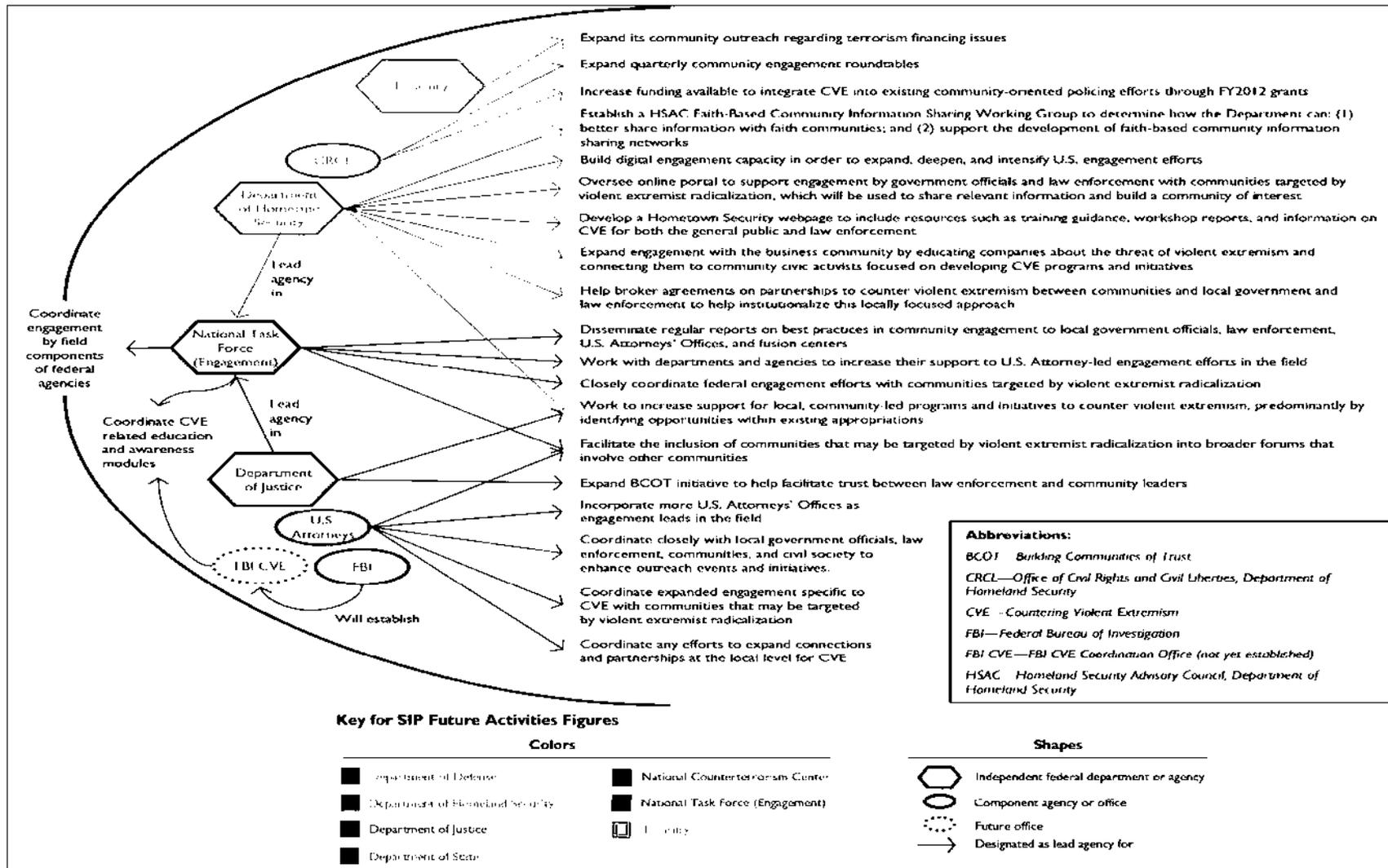
The SIP lists “future activities and efforts” under its three objectives. **Figure 2**, **Figure 3**, and **Figure 4** each cover a single SIP objective. They depict the lead federal agencies responsible for the future activities and efforts subsumed by the relevant objective, and more than one agency can serve as a lead for a particular effort. For the sake of clarity, the figures do not depict partner agencies playing secondary roles and assisting the lead agencies in particular activities. The language used for each of the future activities and efforts in the three figures extensively paraphrases or directly quotes the language used in the SIP. Additionally, the three figures do not include all of the component agencies of specific executive departments. Only the component agencies responsible for future activities and efforts under each SIP objective are included.

Is DHS the De Facto U.S. CVE Lead Agency?

It appears that DHS is cited as a lead agency in 43 of the 62 future activities and efforts discussed in the SIP.¹⁰⁹ Because it is a key player and decision maker in more than two-thirds of the SIP’s impending plans, it seems that DHS may be the de facto lead agency in charge of U.S. CVE activity in the near future. This suggests a critical issue: while granted a large amount of responsibility for implementation of the CVE strategy, will DHS have a matching level of say in its further evolution?

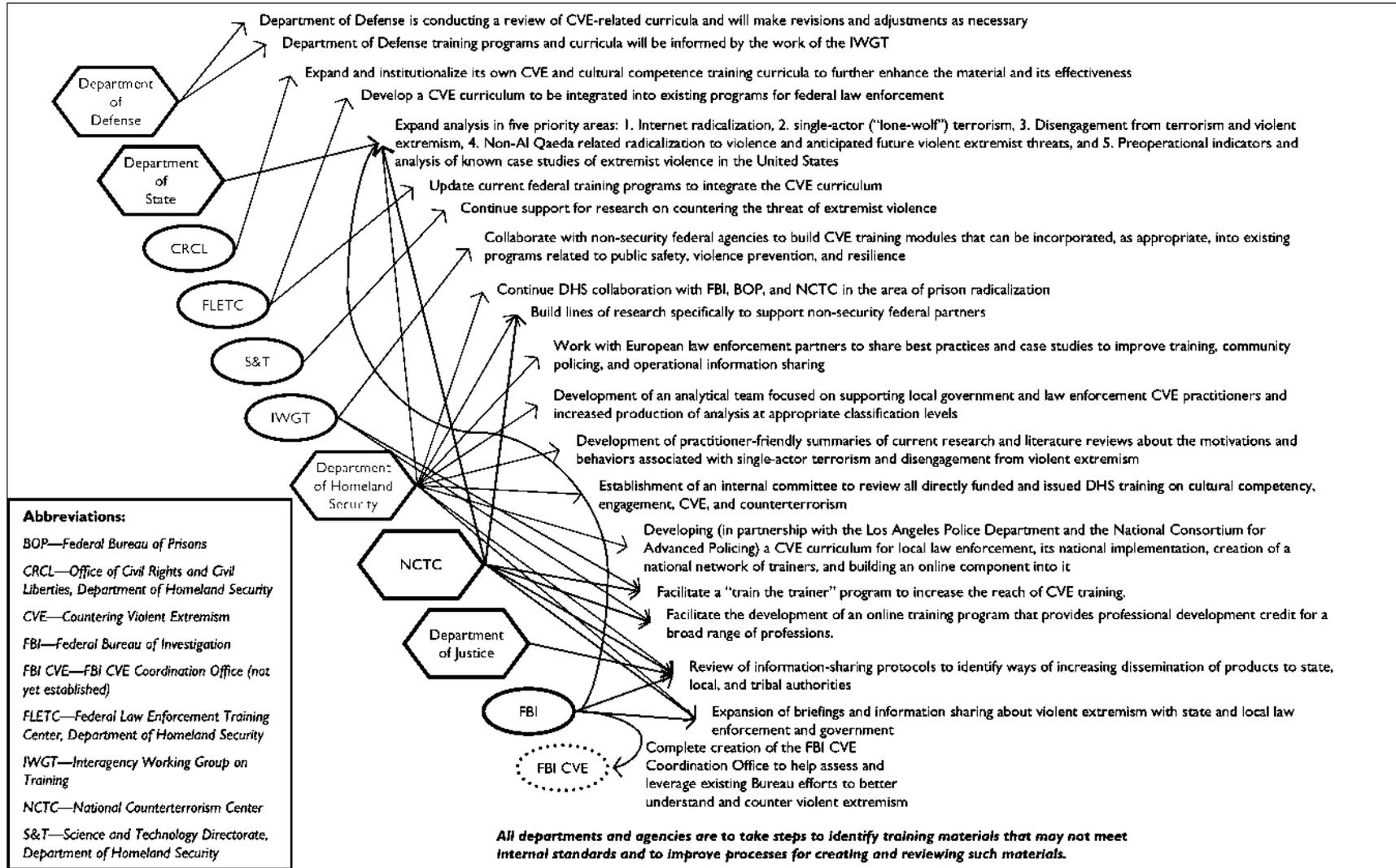
¹⁰⁹ This count includes four responsibilities given to the National Task Force for engagement under the SIP. Both DHS and DOJ are lead agencies in the task force.

Figure 2. Lead Agencies and Their “Future Activities and Efforts” for SIP Objective I, Enhancing Federal Engagement and Support to Local Communities that may be Targeted by Violent Extremists



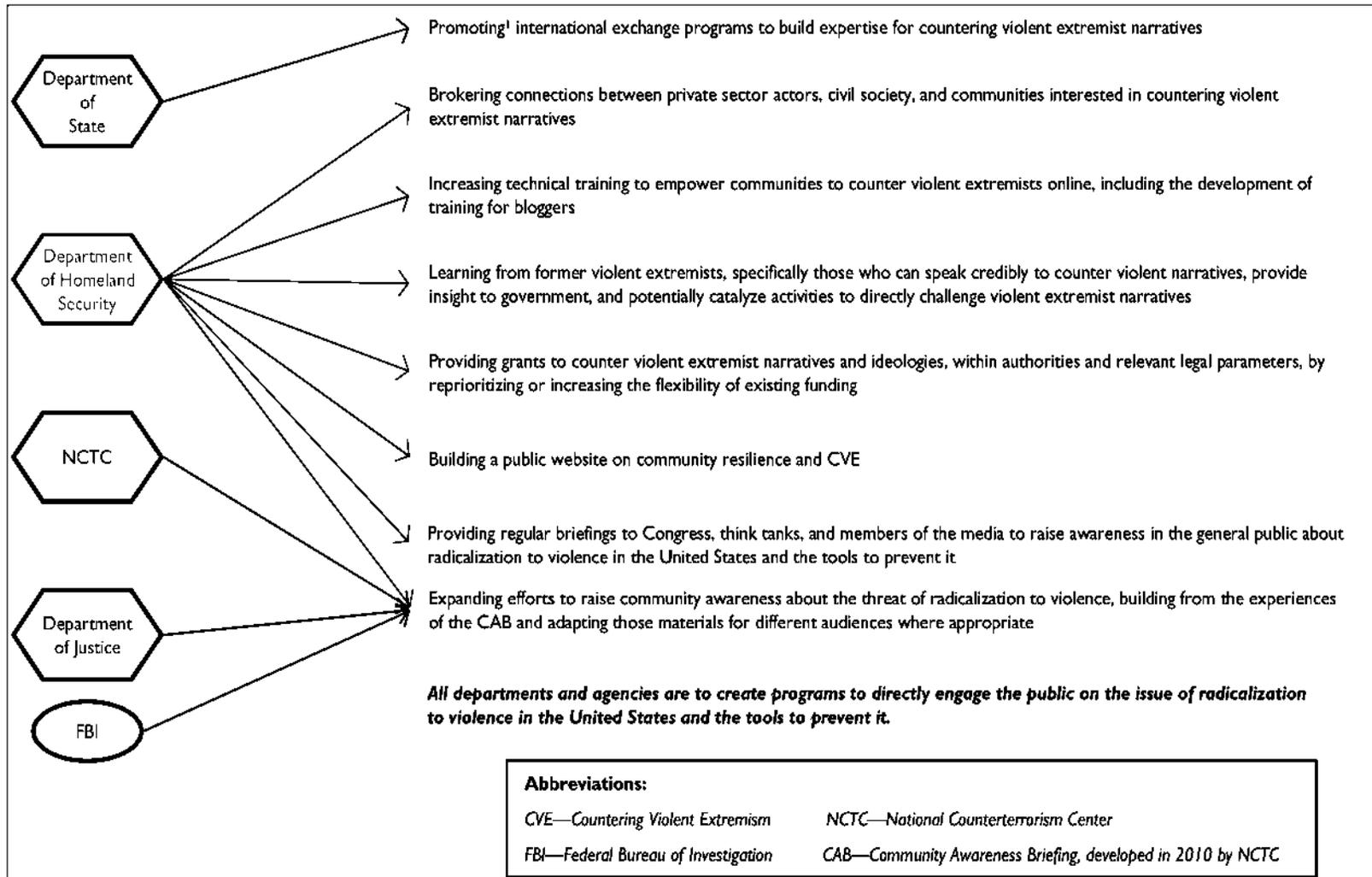
Source: CRS, based on materials contained in the SIP.

Figure 3. Lead Agencies and Their “Future Activities and Efforts” for SIP Objective 2, Building Government and Law Enforcement Expertise for Preventing Violent Extremism



Source: CRS, based on materials contained in the SIP.

Figure 4. Lead Agencies and Their “Future Activities and Efforts” for SIP Objective 3, Countering Violent Extremist Propaganda While Promoting U.S. Ideals



Source: CRS, based on materials contained in the SIP.

Notes: The text in Figure 4 shifts to the present progressive tense, as does the text in the SIP related to the future activities and efforts for Objective 3.

Possible Policy Considerations for Congress

“The United States has made great strides,” says one federal counterterrorism official, “in what might be called tactical counterterrorism—taking individual terrorists off the streets, and disrupting cells and their operations ... an effective counterterrorism strategy must go beyond this ... (to address) the threat of violent extremism.”¹¹⁰ With the announcement of the CVE strategy, the Obama Administration has begun to address this concern. These Administration efforts may attract greater oversight from Congress, especially because the strategy involves the interplay between the public marketplace of ideas involving constitutionally protected activity and the secretive operational realm where terrorists plot and law enforcement pursues.

Implementing the CVE Strategy

As mentioned elsewhere in this report, federal CVE activity emphasizes engagement with Muslim communities across the country. It broadly recognizes this, training, and counter messaging as key components of CVE. However, aside from embracing robust outreach and training for government agencies, the strategy lacks specific initiatives to combat radicalization at the grass-roots level. This suggests a number of other issues.

Picking Partners and Establishing “Rules of the Road”

Who speaks for diverse Muslim communities in America? As mentioned above, “[w]hen asked which of a list of national Muslim-American organizations represents their interests, 55% of Muslim men and 42% of Muslim women say that none do.”¹¹¹ Perhaps sentiments are clearer at the local level, however, these figures suggest the difficulty of selecting partners who accurately represent community needs. It is difficult to speak of one Muslim “constituency” in the United States. The 2.75 million Muslims in the United States have divergent sectarian points of view, come from many ethnic or national backgrounds, and live in a variety of areas. Muslim Americans support many secular and religious organizations.¹¹²

What criteria will the Administration employ in its selection efforts, and how transparent will the process be? Once approved as partners, what “rules of the road” will govern continued cooperation? In essence, what would have to happen for a Muslim community group to fall out of favor with the government? Ad hoc decision making might cause the whole CVE outreach process to appear arbitrary to some community participants. Congress may consider requiring the Administration to release public guidelines in this area. Public guidelines may be especially important, because engagement directly involves engaging people and issues in the open marketplace of ideas and protected constitutional activity.

¹¹⁰ Robert F. Godec, Principal Deputy Director for Counterterrorism at the Department of State, “U.S. Counterterrorism Policy,” an address before the Global Young Leaders Conference, Washington, DC; June 30, 2010, <http://www.state.gov/s/ct/rls/rm/2010/143809.htm>.

¹¹¹ *Muslim Americans: Faith, Freedom, and the Future*, p. 25.

¹¹² Qamar-ul Huda, *The Diversity of Muslims in the United States: Views as Americans*, United States Institute of Peace, Special Report 159, Washington, DC, February 2006. <http://www.usip.org/files/resources/sr159.pdf>. See also: Pew Research Center, *Muslim Americans: No Signs of Growth in Alienation or Support for Extremism*, August 2011, pp. 13-21, <http://www.people-press.org/files/legacy-pdf/Muslim-American-Report.pdf>.

Intervention with At-Risk Individuals

There appears to be little federally driven guidance to community groups on how to intervene with people vulnerable to radicalization.¹¹³ Such an intervention effort, the Channel Program, has been a key element of the United Kingdom's counter radicalization strategy since 2007. The British government describes Channel as a "multi-agency programme to identify and provide support to people at risk of radicalisation" and involvement in "all forms of terrorism."¹¹⁴ Channel "relies on close collaboration between police, partners and other key stakeholders ... and where necessary, provides an appropriate support package tailored to an individual's needs."¹¹⁵ Copying the Channel program in its entirety may not be appropriate for the U.S. context. However, it is unclear whether the Obama Administration considers some variant of Channel workable or even necessary in the United States.

The U.S. CVE strategy does cite the Office of Juvenile Justice and Delinquency Prevention (OJJDP) Comprehensive Gang Model as an example of "locally-based initiatives that connect communities and government to address community challenges through collaboration and the development of stakeholder networks."¹¹⁶ OJJDP—a component of DOJ's Office of Justice Programs—describes the model as "one of the few approaches to gangs that encompasses a multidisciplinary response to gangs on multiple levels."¹¹⁷ The preventative model is intended as a blueprint for organizing local counter-gang efforts that do not necessarily result in law enforcement-driven outcomes, such as investigations, arrests, and prosecutions. For intervention, it targets young adult and teen gang members, not entities such as hate groups, prison gangs, or ideologically driven gangs consisting of adults.¹¹⁸ The model involves five strategies:

Community Mobilization: Involvement of local citizens, including former gang members and community groups and agencies, and the coordination of programs and staff functions within and across agencies.

Opportunities Provision: The development of a variety of specific education, training, and employment programs targeting gang-involved youth.

Social Intervention: Youth-serving agencies, schools, street outreach workers, grassroots groups, faith-based organizations, law enforcement agencies, and other criminal justice organizations reaching out and acting as links between gang-involved youth and their families, the conventional world, and needed services.

Suppression: Formal and informal social control procedures, including close supervision or monitoring of gang youth by agencies of the criminal justice system and also by community-based agencies, schools, and grassroots groups.

¹¹³ Aside from general mention in the *Strategic Implementation Plan*, p. 10.

¹¹⁴ *Prevent Strategy*, p. 54.

¹¹⁵ Association of Chief Police Officers, *National Channel Referral Figures*, <http://www.acpo.police.uk/ACPOBusinessAreas/PREVENT/NationalChannelReferralFigures.aspx>.

¹¹⁶ *Empowering Local Partners*, p. 4.

¹¹⁷ OJJDP, *OJJDP Comprehensive Gang Model: Planning for Implementation*, May 2009, p. 2. Hereinafter: OJJDP, *Comprehensive Gang Model*.

¹¹⁸ OJJDP, *Comprehensive Gang Model*, p. 6.

Organizational Change and Development: Development and implementation of policies and procedures that result in the most effective use of available and potential resources to better address the gang problem.¹¹⁹

The model is designed to focus on youth active in gangs or those who exhibit factors indicating potential gang involvement. It also advocates engagement with the families of such youth. Among its many suggestions, the model discusses interventions such as job training, employment, family counseling, academic tutoring, and anger management classes for young people at-risk. It also calls on law enforcement agencies and courts to move beyond traditional roles in the suppression of gangs—urging them to consider more intervention-oriented activities such as referring youth to social service programs.¹²⁰

The CVE strategy provides little detail about how the Comprehensive Gang Model may be applied to keep vulnerable people from radicalizing and becoming terrorists. Congress may consider examining the utility and feasibility of developing a CVE intervention model for the United States. While elaborating the specific details of such a program may be best left to the federal agencies potentially involved, broadly and publicly exploring what shape it would take might be of value to Congress. Key questions may involve issues such as (1) which agencies would take the lead in creating a program based on the Comprehensive Gang Model? (2) how would the FBI have to adapt its counterterrorism mission—strictly focused on investigating and disrupting terrorist activity—to handle the notion of “social intervention” as suggested by the Comprehensive Gang Model?

Identifying Programs and Federal Contacts to Assist Grassroots CVE Efforts

The Administration’s CVE strategy stresses that “the best defenses against violent extremist ideologies are well-informed and equipped families, local communities, and local institutions.”¹²¹ Determining and explaining how local entities—whether public or private—should interact with federal partners may pose quite a challenge. For example, are there existing federal grant programs that can be harnessed by local actors to develop a CVE intervention program? A publicly available comprehensive list of grant programs that can be harnessed for CVE activities does not exist. Congress may opt to consider the feasibility or the value of such a list or a clearinghouse available to local entities to identify such programs. By possibly pursuing this, Congress may help to ensure that local constituents have better information about and more direct access to federal CVE programs. On the other hand, such a list may be perceived as an additional layer of bureaucracy between constituents and grant programs.

Countering Extremist Ideas: Choosing Good vs. Bad

As the United Kingdom has clearly stated in its counter-radicalization program, extremist ideologies play a role in radicalization.¹²² Furthermore, the National Security Council’s Quintan

¹¹⁹ National Gang Center, “About the OJJDP Comprehensive Gang Model,” <http://www.nationalgangcenter.gov/Comprehensive-Gang-Model/About>. “Suppression” was not emphasized in the Obama Administration’s national CVE strategy’s description of the Comprehensive Gang Model. The other components of the model were mentioned. See *Empowering Local Partners*, p. 4.

¹²⁰ OJJDP, *Comprehensive Gang Model*, p. 6.

¹²¹ *Empowering Local Partners*, p. 2.

¹²² *Prevent Strategy*, p. 7.

Wiktorowicz has commented that “we [the United States] will push back against the full scope of different violent ideologies with an inclusive, positive narrative.”¹²³ However, in the United States, mere belief in radical notions, no matter how reprehensible they are, is not necessarily illegal. The American Civil Liberties Union’s (ACLU’s) Michael German has stated that the ACLU is “deeply concerned about the potential for government censorship of Internet content based on the [CVE] strategy’s proposal for countering violent extremist propaganda.”¹²⁴

Even more fundamentally, the task of countering extremist ideas raises key issues regarding the implementation of the CVE strategy. In the SIP, the Administration notes that when countering violent extremist propaganda, “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.”¹²⁵ This begs the question: do the strategy and the SIP place the federal government in the business of determining which ideologies are dangerous and which are safe—essentially determining which beliefs are good and which are bad? This can be viewed from two angles. One involves establishing parameters for engagement with local communities, the other involves evaluating the end product of engagement, the counter-narrative.

- First, while the SIP may suggest that the government *should not* be involved in *creating* alternatives to violent extremist propaganda, it appears to assume that the government *will* be involved in *sifting* between dangerous and safe ideas—establishing parameters for engagement on this issue. Without picking and choosing between good and bad ideologies, “empowering” local activists to counter specific concepts may prove difficult. Empowering individuals and groups to counter un-named, un-described concepts may prove challenging.
- Second, if the framing of a counter-narrative challenging terrorist ideologies is necessary, how precisely should the federal government partner with state and local government and civilian counterparts in the development of this counter-narrative? How do government entities keep a counter-narrative from being publicly viewed as propaganda or fueling terrorist conspiracy theories about the United States?

Oversight in this area may be vital. As a start, Congress may wish to ask the Administration to better define what it means when referring to “violent extremist narratives.”

The Lack of a Lead Agency

There is no designated single lead agency for any of the three objectives laid out in the SIP. Likewise, there is no single agency managing all of the individual activities and efforts of the plan. At the national level, it arguably may be of value to have a single federal agency in charge of the government’s CVE efforts. One expert has stated as much:

¹²³ Dina Temple-Raston, “White House Unveils Counter-Extremism Plan,” *NPR*, August 3, 2011, <http://www.npr.org/2011/08/04/138955790/white-house-unveils-counter-extremism-plan>.

¹²⁴ “ACLU Lens: Obama Plan to Fight Violent Extremism a Step in the Right Direction, But...” *ACLU Blog of Rights*, August 3, 2011, <http://www.aclu.org/blog/national-security/aclu-lens-obama-plan-fight-violent-extremism-step-right-direction>.

¹²⁵ *Strategic Implementation Plan*, p. 18.

The White House should designate a single agency that serves as the principal hub for collecting, disseminating, and evaluating information on counter-radicalization. Its main function would be to collect, analyze, and share best practices with a wide range of governmental and non-governmental actors, including community leaders and non-profits.¹²⁶

Without a lead agency it may be difficult to monitor the levels of federal funding devoted to CVE efforts. How many personnel are devoted to CVE in the federal government? For how many of these employees is counter radicalization a full-time job? Are there mechanisms to track federal CVE expenditure? Which federal body is responsible for this? Very specifically, the lack of a lead agency is reflected in the fact that DOJ, DHS, and FBI have each issued training guidelines for CVE. They are very similar, but the issuance of three almost identical but separate guidelines raises the question: why not just have one set created by one body overseeing the CVE program? Congress may pursue with the Administration the feasibility or value of designating a lead agency, or the possibility of naming a lead via legislation. However, it is unclear what types of authority—especially in the budgetary realm—such a lead may be able to wield over well-established agencies playing central roles in the CVE strategy.

Measuring Input and Results

On the other side of these budgetary questions, without a lead agency, how will the Administration evaluate the effectiveness of federal CVE efforts? The SIP underscores that individual departments and agencies involved in CVE “will be responsible for assessing their specific activities in pursuit of SIP objectives, in coordination with an Assessment Working Group.”¹²⁷ While this may seem straight-forward, the British government has struggled with measurement issues related to its counter-radicalization strategy. U.K. officials have made “progress ... in measuring outputs but not always in measuring outcomes.”¹²⁸ In other words, counting the number of engagement events is one thing. It is quite another thing to evaluate their impact. The SIP mentions this problem as well.¹²⁹ However, the SIP does not discuss (1) specific metrics, (2) what real authority the Assessment Working Group will have to *independently* evaluate and impact CVE activity within federal departments and agencies, and (3) whether the Assessment Working Group will have the power to standardize measures of success across federal agencies and departments. In the end, the lack of a lead agency with budgetary control over CVE efforts and clear responsibility for implementation of the strategy makes it difficult to conceptualize exactly how spending in this area will be prioritized, evaluated, and then re-prioritized based on results.

Secretiveness vs. Transparency

Without a high degree of transparency, an engagement strategy driven by federal agencies charged with intelligence gathering and law enforcement responsibilities may run the risk of being perceived as an effort to co-opt communities into the security process—providing tips, leads, sources, and informants. This threatens to “securitize” a relationship intended as outreach within the marketplace of ideas. It has been noted that “unlike counterterrorism, which targets

¹²⁶ Neumann, *Preventing Violent Radicalization*, p. 41.

¹²⁷ *Strategic Implementation Plan*, p. 6.

¹²⁸ *Prevent Strategy*, p. 36.

¹²⁹ *Strategic Implementation Plan*, p. 6.

terrorists, counter-radicalization is focused on the communities that are targeted by terrorists for recruitment. The aim is to protect, strengthen, and empower these communities so that they become resilient to violent extremism.”¹³⁰ As such, some suggest that it might not be particularly effective to have the same federal agencies responsible for counterterrorism also be the main players in the CVE strategy.¹³¹ The SIP rejects this notion, stressing that “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.”¹³² The strategy relies on agencies whose enforcement and intelligence missions are undergirded by secretiveness. As it stands, 19 of the 20 “future activities and efforts” for SIP objective 1, which focuses on community engagement, have DOJ, DHS, or a national task force headed by DOJ and DHS as lead agencies. The lone remaining future activity/effort is headed by the Department of Treasury and is focused on terrorism financing, an area of enforcement for the Department.

The fact that DOJ, DHS, and Treasury are key counterterrorism agencies may make it difficult for community groups to view them as full partners, especially if community confidence in them is shaky to start. According to a 2011 study, American Muslims have less confidence than other faith groups in the FBI—“60% of Muslim Americans saying they have confidence in the FBI, versus 75% or more of Americans of other faiths who say this.”¹³³ Because of this reality, Congress may decide to assess whether there is a need for greater transparency from the Administration in its CVE efforts.

Author Contact Information

Jerome P. Bjelopera
Specialist in Organized Crime and Terrorism
jbjelopera@crs.loc.gov, 7-0622

¹³⁰ Neumann, *Preventing Violent Radicalization*, p. 7.

¹³¹ *Ibid.*, p. 8.

¹³² *Strategic Implementation Plan*, p. 4.

¹³³ *Muslim Americans: Faith, Freedom, and the Future*, p. 23.



Countering Violent Extremism in the United States

Jerome P. Bjelopera
Specialist in Organized Crime and Terrorism

May 31, 2012

Congressional Research Service

7-5700

www.crs.gov

R42553

CRS Report for Congress

Prepared for Members and Committees of Congress

DHS-001-425-002563

Page 1 of 33

Summary

In August 2011, the Obama Administration announced its counter-radicalization strategy. It is devised to address the forces that influence some people living in the United States to acquire and hold radical or extremist beliefs that may eventually compel them to commit terrorism. This is the first such strategy for the federal government, which calls this effort “combating violent extremism” (CVE). Since the Al Qaeda attacks of September 11, 2001, the U.S. government has prosecuted hundreds of individuals on terrorism charges. Unlike the necessarily *secretive* law enforcement and intelligence efforts driving these investigations, the CVE strategy includes sizeable government activity within the *open marketplace of ideas*, where private citizens are free to weigh competing ideologies and engage in constitutionally protected speech and expression. Some of the key challenges in the implementation of the CVE strategy likely spring from the interplay between the marketplace of ideas and the secretive realm encompassing law enforcement investigations and terrorist plotting.

The strategy addresses the radicalization of all types of potential terrorists in the United States but focuses on those inspired by Al Qaeda. To further elaborate this strategy, in December 2011 the Administration released its “Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States” (SIP). The SIP is a large-scale planning document with three major objectives and numerous future activities and efforts. The SIP’s three objectives involve (1) enhancing federal community engagement efforts related to CVE, (2) developing greater government and law enforcement expertise for preventing violent extremism, and (3) countering violent extremist propaganda.

This report provides examples of recent Administration CVE activity and examines some of the risks and challenges evident in the SIP’s three objectives. The report also diagrams and briefly discusses the “future activities and efforts” outlined in the SIP for each of these three objectives. *A number of areas may call for oversight from Congress. These include the following:*

Picking Partners and Establishing “Rules of the Road”

Much of the federal government’s CVE effort centers on engagement with Muslim American community groups. This may not be as easy as simply reaching out to local organizations. Who speaks for diverse Muslim communities in America? What criteria will the Administration employ in its selection efforts, and how open will the process be? Once approved as partners, what “rules of the road” will govern continued cooperation? Ad hoc and opaque decision making might render the whole CVE outreach process arbitrary to some community participants. Congress may opt to consider whether there is a need to require the Administration to release public guidelines in this area.

Intervention with At-Risk Individuals

There appears to be little federally driven guidance to community groups on how to intervene with people vulnerable to radicalization. Congress may desire to require the Administration to examine the utility and feasibility of developing a CVE intervention model—possibly akin to gang intervention models—for the United States.

Identifying Programs to Assist Grassroots CVE Efforts

Working with communities entails informing them of possible resources they can use. A publicly available, comprehensive list of grant programs that can be harnessed for CVE activities does not exist. Congress may be interested in asking the Administration to formalize a roster or designate a clearinghouse available to local entities to identify such programs. By possibly pursuing this, Congress may help to ensure that local constituents have better information about and more direct access to federal CVE programs. On the other hand, such a list could be perceived as an additional layer of bureaucracy between constituents and grant programs.

Countering Extremist Ideas: Choosing Good vs. Bad

The task of countering extremist ideas highlighted in the CVE strategy and SIP raises a number of questions. Do the strategy and the SIP place the federal government in the business of determining which ideologies are dangerous and which are safe—essentially determining which beliefs are good and which are bad? In order to conduct effective oversight, Congress may choose to ask the Administration to define exactly what it means when referring to “violent extremist narratives.”

The Lack of a Lead Agency

There is no single agency managing all of the individual activities and efforts of the plan. At the national level, some may argue that it would be of value to have a single federal agency in charge of the government’s CVE efforts. From their perspective, without a lead agency it may be difficult to monitor the levels of federal funding devoted to CVE efforts and how many personnel are devoted to CVE in the federal government. For how many of these employees is counter-radicalization a full-time job? Are there mechanisms to track federal CVE expenditure? Which federal body is responsible for this? Congress may wish to pursue with the Administration the feasibility or value of designating a lead agency, or the possibility of naming a lead via legislation. However, it is unclear what types of authority—especially in the budgetary realm—such a lead may be able to wield over well-established agencies playing central roles in the CVE strategy.

Transparency

Without a high degree of transparency, an engagement strategy driven by federal agencies charged with intelligence gathering and law enforcement responsibilities may run the risk of being perceived as an effort to co-opt communities into the security process—providing tips, leads, sources, and informants. Some may maintain that this threatens to “securitize” a relationship intended as outreach within the marketplace of ideas. As such, critics may argue that it might not be particularly effective to have the same federal agencies responsible for classified counterterrorism investigations grounded in secrecy also be the main players in the CVE strategy. However, the Department of Homeland Security, the Department of Justice, and the Federal Bureau of Investigation have responsibilities for much of the CVE program. Because of this reality, Congress may opt to consider whether there is a need for greater transparency from the Administration in its CVE efforts.

Contents

Introduction: Counterterrorism Context	1
From Radicalization to Terrorism.....	3
Countering Radicalization in the United States	4
Administration Strategy and Current Activities	4
Community Engagement.....	5
Risks and Challenges	9
Building Government and Law Enforcement Expertise	14
Risks and Challenges	17
Countering Violent Extremist Propaganda.....	18
Risks and Challenges	19
Administration Plan and Future Activities	19
Is DHS the De Facto U.S. CVE Lead Agency?.....	20
Possible Policy Considerations for Congress	24
Implementing the CVE Strategy.....	24
Picking Partners and Establishing “Rules of the Road”.....	24
Intervention with At-Risk Individuals.....	25
Identifying Programs and Federal Contacts to Assist Grassroots CVE Efforts	26
Countering Extremist Ideas: Choosing Good vs. Bad.....	26
The Lack of a Lead Agency	27
Secretiveness vs. Transparency	28

Figures

Figure 1. Counterterrorism Context.....	2
Figure 2. Lead Agencies and Their “Future Activities and Efforts” for SIP Objective 1, <i>Enhancing Federal Engagement and Support to Local Communities that may be Targeted by Violent Extremists</i>	21
Figure 3. Lead Agencies and Their “Future Activities and Efforts” for SIP Objective 2, <i>Building Government and Law Enforcement Expertise for Preventing Violent Extremism</i>	22
Figure 4. Lead Agencies and Their “Future Activities and Efforts” for SIP Objective 3, <i>Countering Violent Extremist Propaganda While Promoting U.S. Ideals</i>	23

Contacts

Author Contact Information.....	29
---------------------------------	----

Introduction: Counterterrorism Context

In August 2011, the Obama Administration released its domestic counter-radicalization strategy. The Administration dubbed this effort “countering violent extremism” (CVE).¹ Implementation of the CVE strategy revolves around impeding the radicalization of violent jihadists in the United States.² As this may suggest, for this report, a couple of concepts are key. Namely, “radicalization” describes the process of acquiring and holding radical or extremist beliefs; and “terrorism” describes violent or illegal action taken on the basis of these radical or extremist beliefs.

This report examines the implementation of the Administration’s counter-radicalization strategy and provides possible policy considerations for Congress relating to this relatively new area of coordinated federal activity. Implementation of the CVE strategy involves many elements within the executive branch and brushes against a number of key issues involving constitutionally protected activity versus effective counterterrorism policing efforts.

Government-related efforts to stave off terrorist activity in the United States exist within two broad contexts. First, the operational aspects of violent terrorist plots largely involve clandestine illegal activity. Since the terrorist attacks of September 11, 2001 (9/11), hundreds of individuals have been implicated in more than 50 homegrown violent jihadist plots or attacks.³ In this *secretive realm*, law enforcement pursues terrorists in a real-world version of hide-and-seek. Domestic law enforcement strategies devised in the decade since 9/11 to prevent terrorism largely focus their efforts in this area.⁴ Federal law enforcement activity in this arena is geared toward rooting out terrorists and stopping them from successfully executing their plots.

¹ *Empowering Local Partners to Prevent Violent Extremism in the United States*, August 2011, p. 1, http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf. Hereafter: *Empowering Local Partners*.

² The Obama Administration recognized the significance of the homegrown jihadist threat in its June 2011 *National Strategy for Counterterrorism*. This strategy document focuses on Al Qaeda, its affiliates (groups aligned with it), and its *adherents* (individuals linked to or inspired by the terrorist group). John Brennan, President Obama’s top counterterrorism advisor, publicly described the strategy as the first one, “that designates the homeland as a primary area of emphasis in our counterterrorism efforts.” See White House, *National Strategy for Counterterrorism*, June 2011, http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf; Mathieu Rabecchault, “U.S. Refocuses on Home-Grown Terror Threat,” *AFP*, June 29, 2011, <http://www.google.com/hostednews/afp/article/ALeqM5hLyJyB7khhqJxWOOlm1mCj7IYsRQ?docId=CNG.3f90005700ea65e0b05509a135c7a3a8.471>; Karen DeYoung, “Brennan: Counterterrorism Strategy Focused on al-Qaeda’s Threat to Homeland,” *Washington Post*, June 29, 2011, http://www.washingtonpost.com/national/national-security/brennan-counterterrorism-strategy-focused-on-al-qaedas-threat-to-homeland/2011/06/29/AGki1LrH_story.html.

³ See CRS Report R41416, *American Jihadist Terrorism: Combating a Complex Threat*, by Jerome P. Bjelopera. For lists of individuals involved in terrorism cases see <http://homegrown.newamerica.net/table>; “Profiles in Terror,” <http://motherjones.com/fbi-terrorist>. For this CRS report, “homegrown” describes terrorist activity or plots perpetrated within the United States or abroad by American citizens, legal permanent residents, or visitors radicalized largely within the United States. “Jihadist” describes radicalized Muslims using Islam as an ideological and/or religious justification for belief in the establishment of a global caliphate—a jurisdiction governed by a Muslim civil and religious leader known as a caliph—via violent means. Jihadists largely adhere to a variant of Salafi Islam—the fundamentalist belief that society should be governed by Islamic law based on the Quran and follow the model of the immediate followers and companions of the Prophet Muhammad. For more on Al Qaeda’s global network, see CRS Report R41070, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*, coordinated by John Rollins.

⁴ For more information on federal counterterrorism law enforcement, see CRS Report R41780, *The Federal Bureau of Investigation and Terrorism Investigations*, by Jerome P. Bjelopera.

The second context is the open *marketplace of ideas*. Here, private citizens are free to weigh competing ideologies and engage in constitutionally protected speech and expression. In this arena, a relative few ordinary law-abiding persons move from the mainstream and adopt radical ideologies that embrace terrorism. As they radicalize, *they do not necessarily commit crimes*. Much like the policing that occurs in the secretive realm, the federal government’s CVE strategy is a preventative approach to terrorism, *but it is not wholly focused on policing*. Rather, federal activity in this arena is geared toward helping local communities and individuals boost their resilience to terrorist radicalization efforts.

The divergent nature of these two contexts may imply clear distinction between the marketplace of ideas and the secretive operational realm. In reality, they are far from distinct. What happens operationally has significant impacts in the marketplace of ideas (**Figure 1**). This interrelationship is highlighted by any number of issues. For example,

- the success of terrorist plots in the secretive realm may spur radicalization and generate public fear in the marketplace of ideas;
- conversely, successful investigations in the secretive realm may discourage radicalizing individuals within the marketplace of ideas from eventually embracing violent acts of terrorism as an ultimate goal;
- effective policing within the secretive realm may depend on a trusting community acting supportively in the marketplace of ideas;
- perceived policing excesses in the secretive realm may impede community engagement with law enforcement; and
- high levels of radicalization occurring in the marketplace of ideas may expand the potential pool of terrorist recruits, while an effective government strategy to counter radicalization may staunch terrorist recruitment.

Figure 1. Counterterrorism Context



Source: CRS.

In fact, some of the key challenges involved in implementing a national strategy to deal with terrorist radicalization spring from the interplay between the marketplace of ideas and the secretive realm.

From Radicalization to Terrorism

A key way to fight the threat of homegrown terrorists is to develop an understanding of how radicalization works and formulate ways to prevent radicalization from morphing into terrorist plotting. In 2007, the New York City Police Department's (NYPD) Intelligence Division released a study of domestic jihadist radicalization that has been widely circulated within the law enforcement community.

The NYPD study describes a general four-step process of radicalization leading to terrorist plotting. First, individuals exist in a pre-radicalization phase in which they lead lives unaware of or uninterested in either violent jihad or fundamentalist Salafi Islam. Next, they go through self-identification in which some sort of crisis or trigger (job loss, social alienation, death of a family member, international conflict) urges them to explore Salafism. Third, individuals undergo indoctrination or adoption of jihadist ideals combined with Salafi views. The study indicates that, typically, a "spiritual sanctioner" or charismatic figure plays a central role in the indoctrination process. Finally, radicalizing individuals go through "jihadization," where they identify themselves as violent jihadists, and are drawn into the planning of a terrorist attack.⁵ At this point, according to the NYPD, they can be considered violent extremists (terrorists). The Federal Bureau of Investigation's (FBI) own four-stage model of radicalization closely follows that of the NYPD.⁶

This model and the process it describes—though useful—should, however, be read with caution, according to some observers. The radicalization process is best depicted in broad brush strokes. Brian Michael Jenkins has suggested that

There is no easily identifiable terrorist-prone personality, no single path to radicalization and terrorism. Many people may share the same views, and only a handful of the radicals will go further to become terrorists. The transition from radical to terrorist is often a matter of happenstance. It depends on whom one meets and probably on when that meeting occurs in the arc of one's life.⁷

Some experts have warned against viewing the radicalization process as a "conveyor belt," somehow starting with grievances and inevitably ending in violence.⁸ The NYPD report itself acknowledges that individuals who begin this process do not necessarily pass through all the stages nor do they necessarily follow all the steps in order, and not all individuals or groups who

⁵ Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, City of New York Police Department, Intelligence Division, New York, 2007, pp. 6-8, http://sethgodin.typepad.com/seths_blog/files/NYPD_Report-Radicalization_in_the_West.pdf. Hereafter: Silber and Bhatt, *Radicalization in the West*.

⁶ Carol Dyer, Ryan E. McCoy, Joel Rodriguez, et al., "Countering Violent Islamic Extremism: A Community Responsibility," *FBI Law Enforcement Bulletin*, December 2007, p. 6.

⁷ Brian Michael Jenkins, *Would Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001* (Santa Monica, CA: The RAND Corporation, 2010), p. 7.

⁸ Sophia Moskalenko and Clark McCauley, "Measuring Political Mobilization: The Distinction Between Activism and Radicalism," *Terrorism and Political Violence*, vol. 21, no. 2 (April 2009), pp. 239-240.

begin this progression become terrorists.⁹ Studies by the Department of Homeland Security's (DHS) Office of Intelligence and Analysis indicate that the radicalization dynamic varies across ideological and ethno-religious spectrums, different geographic regions, and socio-economic conditions. Moreover, there are many diverse "pathways" to radicalization and individuals and groups can radicalize or "de-radicalize" because of a variety of factors.¹⁰

In a more fundamental conceptualization, radicalization expert Peter Neumann has noted that three core elements exist in the radicalization process. These are grievance, ideology/narrative, and mobilization.¹¹ Grievances can stem from narrow issues unique to an individual's personal life or arise from broader perceptions of the surrounding world. A radicalizing individual seizes upon extremist ideologies or narratives to help explain his or her grievance. Mobilization consists of an individual acting on his or her grievances based on precepts culled from a particular ideology or narrative. These actions can involve criminality.¹²

Countering Radicalization in the United States

Because so much of the radicalization process occurs within the marketplace of ideas, counter-radicalization efforts involve activity in the same realm. American counter-radicalization approaches favor government engagement with communities affected by terrorism. Scholars who have studied the circumstances that are associated with voluntary cooperation by Muslim-Americans in anti-terror policing efforts have identified strong evidence that when authorities are viewed as more legitimate, their rules and decisions are more likely to be accepted.¹³ Community engagement is—in part—an effort to make law enforcement authority more accepted within localities.

Administration Strategy and Current Activities

The Administration's CVE strategy revolves around countering the radicalization of all types of potential terrorists. As such, the radicalization of violent jihadists falls under its purview and is the key focus. The initial August 2011 strategy was supported by the Administration's release in December 2011 of its "Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States" (SIP).¹⁴ The SIP is a large-scale planning document with three major objectives and numerous future activities and efforts. There is no single lead agency for any of the three objectives. Likewise, there is no single agency managing all of the individual

⁹ Silber and Bhatt, *Radicalization in the West*, pp. 10, 19.

¹⁰ U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, Written Testimony of Charles E. Allen, Assistant Secretary of Intelligence and Analysis and Chief Intelligence Officer, Department of Homeland Security, "Threat of Islamic Radicalization to the Homeland," 110th Cong., 1st sess., March 14, 2007, p. 5.

¹¹ Ryan Hunter and Danielle Heinke. "Radicalization of Islamist Terrorists in the Western World." *FBI Law Enforcement Bulletin*, (September 2011), pp. 27-29, <http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/september-2011>. Hunter and Heinke rely on the ideas of scholar Peter Neumann.

¹² *Ibid.*

¹³ Tom R. Tyler, Stephen Schulhofer, and Aziz Huq, "Legitimacy and Deterrence Effects in Counter-Terrorism Policing," New York University School of Law, Public Law Research Paper No. 10-15, February 23, 2010, p. 2, http://lsr.nellco.org/cgi/viewcontent.cgi?article=1182&context=nyu_plltwp.

¹⁴ *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States*, December 2011, <http://www.whitehouse.gov/sites/default/files/sip-final.pdf>. Hereafter: *Strategic Implementation Plan*.

future activities and efforts of the plan. The SIP's three objectives or "core areas of activity" are "(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 [U.S.] ideals."¹⁵

The following sections provide examples of recent Administration CVE activity and discussion of the risks and challenges evident in the SIP's three core areas of activity. The "future activities and efforts" outlined for each of the three core areas of activity in the SIP are also diagrammed and briefly discussed below.

Community Engagement

The concept of building trust through engagement and partnership is rooted in the community policing model developed by law enforcement professionals in the 1990s, and community policing is mentioned in the Administration's CVE strategy.¹⁶ Following the 9/11 attacks, law enforcement agencies came to realize the prevention of terrorist attacks would require the cooperation and assistance of American Muslim, Arab, and Sikh communities. "Embedded within these communities," notes Professor Deborah Ramirez, "are the linguistic skills, information, and cultural insights necessary to assist law enforcement in its efforts to identify suspicious behavior. In order to have access to these critical tools and information, law enforcement recognized the need to build bridges required for effective communication with these groups."¹⁷ At the same time, Muslim, Arab, and Sikh Americans recognized the need to define themselves as distinctly American communities who, like all Americans, desire to help prevent another terrorist attack.¹⁸

A study by the Homeland Security Institute found that "[c]ommunity policing has been applied with notable success in places such as New York City, Chicago, Boston, and San Diego, and has been widely adopted (at least in name) throughout the United States."¹⁹ A Homeland Security

¹⁵ Ibid., p. 2.

¹⁶ Ibid., pp. 3, 6. The Justice Department has defined community policing as "a philosophy that promotes organizational strategies, which support the systematic use of partnerships and problem-solving techniques, to proactively address the immediate conditions that give rise to public safety issues such as crime, social disorder, and fear of crime." One of its key features is the establishment of collaborative partnerships between law enforcement agencies and individuals and organizations they serve to develop solutions to problems and increase trust in police. See DOJ Office of Community Oriented Policing Services, *Community Policing Defined*, April 3, 2009, p. 3, <http://www.cops.usdoj.gov/files/RIC/Publications/c030917193-CP-Defined.pdf>.

¹⁷ Deborah A. Ramirez, Sasha Cohen O'Connell, and Rabia Zafar, The Partnering for Prevention and Community Safety Initiative, *A Promising Practices Guide Executive Summary*, 2004, p. 2, http://www.cps.neu.edu/plp/downloads/PPP_Executive_Summary__cover.pdf.

¹⁸ Ibid.

¹⁹ Rosemary Lark (Task Lead), Richard Rowe, and John Markey, *Community Policing Within Muslim Communities: An Overview and Annotated Bibliography of Open-Source Literature*. Homeland Security Institute, December 27, 2006, p. iii. This study, prepared for the DHS Science and Technology Directorate, sought to identify the literature that examined community policing initiatives underway within Muslim Communities in the U.S., and the extent to which they were successful in achieving the objectives of (1) inclusiveness, promoting integration, and potentially minimizing the disaffection that can lead to radicalization, particularly among Muslim youth; (2) serving as early warning to identifying incipient radicalization or terrorist activities; and (3) opening a new channel of communication with individuals who can navigate the linguistic and cultural complexities of Islam, providing needed context to inform intelligence analysis, http://www.homelandsecurity.org/hsireports/Task_06-99_Community_Policing_within_Muslim_Communities.pdf.

Advisory Council (HSAC) working group²⁰ chaired by Maryland Governor Martin O'Malley commented on Community-Oriented Policing, stating that

Effective public-private partnerships, designed to enable civic engagement, problem-solving, and violent crime mitigation provide the foundation for efforts to prevent, protect against and respond to violent criminal activity—including that which may be motivated by ideological objectives.²¹

The Administration's CVE strategy depends on federal agencies cooperating with local groups to expand engagement efforts and to foster preventative programming "to build resilience against violent extremist radicalization...."²² In fact, it highlights a "community-based approach" for the federal government, and much of the activity it describes will take place in the "marketplace of ideas" described in **Figure 1**. To this end, the federal government most effectively acts as a "facilitator, convener, and source of information."²³ Since November 2010, a national task force led by DOJ and DHS has helped coordinate CVE-related community engagement from the national perspective. It works with U.S. Attorneys, DHS's Office for Civil Rights and Civil Liberties (CRCL), the Department of State, and DOJ, among others.²⁴

Role of U.S. Attorneys

Under the Administration's CVE strategy, U.S. Attorneys play a key role in community engagement within their jurisdictions.²⁵ U.S. Attorneys are "the nation's principal litigators under the direction of the Attorney General."²⁶ Attorney General Eric Holder has pushed the U.S. Attorneys to enhance their outreach efforts to Muslim, Sikh, and Arab American communities.²⁷ Within their districts across the country, U.S. Attorneys have met with Muslim communities regarding specific situations and trends.²⁸ In December 2010, DOJ began a pilot program involving U.S. Attorneys in community outreach efforts. This program did not specifically focus on CVE efforts but has included radicalization-related outreach.²⁹ For example, in September

²⁰ HSAC provides advice and recommendations to the Secretary of Homeland Security. The chair of the council is Judge William Webster, former Director of the CIA and Director of the FBI. Other members include leaders from state and local government, first responder communities, the private sector, and academia. The Countering Violent Extremism Working Group originated from a tasking by Secretary Napolitano to the HSAC in February 2010 to work with state and local law enforcement and relevant community groups to develop and provide recommendations on how DHS can better support community-based efforts to combat violent extremism domestically. See Homeland Security Advisory Council, Countering Violent Extremism Working Group, Spring 2010, p. 2. Hereafter: HSAC CVE Working Group, Spring 2010.

²¹ HSAC CVE Working Group, Spring 2010, p. 5.

²² *Strategic Implementation Plan*, p. 10.

²³ *Empowering Local Partners*, p. 3.

²⁴ *Strategic Implementation Plan*, p. 9.

²⁵ *Ibid.*, p. 8.

²⁶ DOJ, "United States Attorneys' Mission Statement," <http://www.justice.gov/usao/about/mission.html>.

²⁷ DOJ, "Arab and Muslim Engagement: U.S. Attorneys' Outreach Efforts," http://www.justice.gov/usao/briefing_room/crt/engagement.html. Hereafter: DOJ, "Arab and Muslim."

²⁸ DOJ, *Ten Years Later: The Justice Department After 9/11, Partnering with the Muslim, Arab, and Sikh Communities*, <http://www.justice.gov/911/partnerships.html>. Hereafter: DOJ, *Ten Years Later*.

²⁹ *Strategic Implementation Plan*, p. 8.

2011, the U.S. Attorney for the District of Oregon and Attorney General Holder met with Arab and Muslim community representatives in Portland, Oregon.³⁰

Comparable outreach has been pursued by other U.S. Attorneys. The District of Minnesota has established the Young Somali-American Advisory Council. This responded to al-Shabaab's³¹ recruitment of young men within the greater Minneapolis-St. Paul, Minnesota Somali community.³² The council includes more than a dozen people between the ages of 18 and 30. Among the outreach activities tied to the council, the U.S. Attorney's office instructed council members on civics issues. In a similar vein, the U.S. Attorney for the Southern District of Florida and Assistant Attorney General Thomas E. Perez met with Muslim and Arab leaders in Miami in February 2011.³³ Likewise, in November 2010, an alleged jihadist terrorist plotter was arrested for purportedly attempting to bomb a Christmas tree lighting ceremony in Portland. In the plot's wake, the state's U.S. Attorney repeatedly met with local Muslim leaders.³⁴

Other Federal Activities

Currently, aside from the special role given to U.S. Attorneys, other elements of DOJ and additional U.S. government agencies engage and partner with Muslim American communities. Some of these efforts by DHS, DOJ, and FBI are detailed below.

Department of Homeland Security

DHS has stated that public outreach to local communities plays a major role in the department's mission.³⁵ Engagement activities are centered in the Office for Civil Rights and Civil Liberties (CRCL), which began its outreach in 2003.³⁶ Its work involves counterterrorism and CVE-related matters, but its overall mission is broader. The office is also responsible for³⁷

- advising DHS leadership, personnel, and partners about civil rights and civil liberties issues;
- communicating with individuals and communities whose civil rights and civil liberties may be affected by DHS activities, informing them about policies and

³⁰ DOJ, "Attorney General Holder Meets with Muslim Leaders in Portland," September 30, 2011, <http://blogs.usdoj.gov/blog/archives/1617?print=1>. Hereafter: DOJ, "Attorney General Holder Meets."

³¹ A terrorist group in Somalia.

³² B. Todd Jones, U.S. Attorney for the District of Minnesota, "Arab and Muslim Engagement: Countering Violent Extremism through Community-Based Approaches," <http://www.justice.gov/usao/mn/oped.html>; Laura Yuen, "Years After Somali Men Left Minn., Youth Decry Extremism," Minnesota Public Radio, November 8, 2011, <http://minnesota.publicradio.org/display/web/2011/11/08/young-minnesota-somalis-decry-extremism/>.

³³ DOJ, "Arab and Muslim."

³⁴ Peter Neumann, *Preventing Violent Radicalization in America*, Bipartisan Policy Center, (June 2011), p. 37 <http://www.bipartisanpolicy.org/sites/default/files/NSPG.pdf>. Hereafter: Neumann, *Preventing Violent Radicalization*.

³⁵ CRCL, "Engagement with Key Communities Team," August 14, 2009. Hereafter: CRCL Engagement Team, August 14, 2009.

³⁶ CRCL, *Newsletter*, vol. 2, no. 1 (September 2011), http://www.aila.org/content/default.aspx?docid_36956. Hereafter: CRCL, *Newsletter*, September 2011.

³⁷ The mission of the DHS Office for Civil Rights and Civil Liberties is outlined in 6 U.S.C. 345, http://www.dhs.gov/about/structure/editorial_0481.shtm. See DHS, Office of Civil Rights and Civil Liberties, <http://www.dhs.gov/about/structure/crcl.shtm>.

- avenues of redress, and promoting appropriate attention within DHS to their experiences and concerns; and
- investigating and resolving civil rights and civil liberties complaints filed by the public.

CRCL has a Community Engagement Section. Recent domestic CVE-related³⁸ outreach events have been coordinated by CRCL and its Community Engagement Section.³⁹

Department of Justice

In addition to the CVE role played by U.S. Attorneys, DOJ's engagement activities largely appear to come from the Civil Rights Division and the Community Relations Service.⁴⁰ According to its website, since the terrorist attacks of September 11, 2001 (9/11), the Civil Rights Division of DOJ has prioritized prosecution of bias crimes and discrimination against Muslims, Sikhs, and persons of Arab and South-Asian descent, as well as individuals perceived to be members of these groups. These types of incidents are commonly referred to as "backlash." The division has also educated people in these communities about their rights and available government services.⁴¹ Senior Civil Rights Division officials have met with Muslim, Sikh, Arab, and South Asian community leaders regarding backlash discrimination issues. Like the Civil Rights Division, DOJ's Community Relations Service is involved in outreach. Since 9/11, the service has held meetings around the country to address backlash-related issues.⁴²

Federal Bureau of Investigation

The FBI has publicly suggested that since 9/11, it has been formulating an "extensive program" to bolster its relationship with Arab, Muslim, Sikh, and South Asian communities in the United States.⁴³ In March 2010, the Chief of the Community Relations Unit of the FBI's Office of Public

³⁸ Much like CRCL, the Section's mission involves more than CVE. It reaches out to other communities whose issues are not necessarily tied to radicalization.

³⁹ CRCL, *Fiscal Year 2010 Annual and Consolidated Quarterly Reports to Congress*, September 20, 2011, pp. 14-15, <http://www.dhs.gov/xlibrary/assets/crcl-annual-report-fy-2010.pdf>; CRCL Engagement Team, August 14, 2009. DHS also provides law enforcement training related to CVE in the United States. With DOJ, DHS has instructed more than 46,000 "front line officers" on suspicious activity reporting. As of September 2011, CRCL taught over 2,000 law enforcement officials in the area of CVE. CRCL CVE training highlights topics such as understanding violent radicalization, cultural awareness, and community engagement. The training was developed "in response to concerns from attendees at community roundtables." See DHS, Fact Sheet, "The Department of Homeland Security's Approach to Countering Violent Extremism," <http://www.dhs.gov/files/fact-sheet-approach-to-countering-violent-extremism.pdf>. Hereafter: DHS, Fact Sheet. See also: CRCL, *Newsletter*, vol. 1, no. 8 (June 2011), <http://www.aila.org/content/default.aspx?docid=36057>.

⁴⁰ DOJ, "Attorney General Holder Meets."

⁴¹ Civil Rights Division, "Initiative to Combat Post-9/11 Discriminatory Backlash," <http://www.justice.gov/crt/legalinfo/discrimupdate.php>. Hereafter: Civil Rights Division, "Initiative."

⁴² *Ibid.*; Community Relations Service, *America's Peacemaker, Community Relations Service, U.S. Department of Justice, Annual Report, Fiscal Year 2010*, <http://www.justice.gov/crs/pubs/annualreport2010.pdf>; DOJ, *Ten Years Later*; Civil Rights Division, "Initiative." See Ondray T. Harris, Director, DOJ Community Relations Service, "Creating Positive Perception of Sikh Identity in the U.S. Public," speech at the 2nd Global Sikh Civil Rights Conference in Toronto, Canada, December 19, 2009, <http://www.justice.gov/crs/united-sikhs.pdf>.

⁴³ Scott Atran, *Senate Armed Services Subcommittee on Emerging Threats and Capabilities: Countering Violent Extremism: Statement for the Record, Addendum-2*, 111th Cong., 2nd scss., March 10, 2010, <http://armed-services.senate.gov/statemnt/2010/03%20March/Atran%2003-10-10.pdf>. Hereafter: Atran Testimony, March 10, 2010.

Affairs testified to Congress that the primary purpose of the agency's outreach program was "to enhance public trust and confidence in the FBI."⁴⁴ This involves fostering a positive image of law enforcement among U.S. organizations that have condemned terrorism and violent radicalization. The FBI relies on programs at the field office level to foster interaction with a wide variety of local groups.⁴⁵ Also, some FBI field offices have formally interacted with local Muslim communities regarding specific cases.⁴⁶ At the national level, FBI headquarters representatives have engaged in liaison with Arab and Muslim American advocacy groups and have regular issue-focused conference calls with community leaders.⁴⁷ The FBI is also a member of the Incident Coordination Communications Team managed by DHS CRCL.

Risks and Challenges

Although there is considerable support among public officials for community engagement, some experts warn of significant challenges in the development of programs that foster substantive relationships rather than token discussions or community relations events. A study of policing in Arab American communities sponsored by the National Institute of Justice, for example, highlighted four key obstacles hindering outreach between U.S. Arabs (Christian and Muslim) and law enforcement: "Distrust between Arab communities and law enforcement, lack of cultural awareness among law enforcement officers, language barriers, and concerns about immigration status and fears of deportation."⁴⁸

Terrorism expert Marc Sageman cautions that engagement can be a sign of government focus on Muslim communities when instead it should be stressed that Muslims are Americans just like everyone else.⁴⁹ He sees another challenge arise when engagement on the government side is led by federal agencies with law enforcement and intelligence responsibilities. "It can send the message that we are only interested in Muslims because they are potential law breakers. No other foreign or religious communities in the United States get this type of scrutiny."⁵⁰

Outreach may be most effective when U.S. Muslim communities initiate it and community-government contact revolves around countering the extremist messages popular among violent jihadists.⁵¹ Marc Sageman also suggests it would be more appropriate for local authorities, such

⁴⁴ Brett Hovington, *House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment: Working with Communities to Disrupt Terror Plots: Statement for the Record*, 111th Cong., 2nd sess., March 17, 2010, <http://homeland.house.gov/SiteDocuments/20100317103507-03554.pdf>. Hereafter: Hovington Testimony, March 17, 2010.

⁴⁵ Hovington Testimony, March 17, 2010. See also: FBI, "Building Trust: The Arab, Muslim, and Sikh Advisory Council." June 1, 2009. <http://washingtondc.fbi.gov/trust060109.htm>.

⁴⁶ Hovington Testimony, March 17, 2010.

⁴⁷ Atran Testimony, March 10, 2010.

⁴⁸ Nicole J. Henderson et al., *Policing in Arab-American Communities After September 11*, National Institute of Justice, Washington, DC, July 2008, p. ii. For the full study, see Nicole J. Henderson et al., *Law Enforcement and Arab American Community Relations After September 11, 2001: Engagement in a Time of Uncertainty*, Vera Institute of Justice, New York, NY, June 2006. <http://www.vera.org/policerelations>. As its title clearly suggests, this project examined the experiences of Arab-Americans, two thirds of whom are Christian.

⁴⁹ Discussion with CRS, April 7, 2010. Sageman is an independent researcher on terrorism, founder of Sageman Consulting, LLC, and author of *Leaderless Jihad: Terror Networks in the Twenty-First Century* (University of Pennsylvania Press, 2008).

⁵⁰ *Ibid.*

⁵¹ Gartenstein-Ross and Grossman, *Homegrown Terrorists in the U.S. and U.K.*, p. 60.

as a mayor's office, to perform the engagement role because they know these communities better than federal officials.

The Tension Between Enforcement and Engagement Activities

An inherent challenge to building trust and partnership involves law enforcement investigative activities and tactics that can be perceived to unfairly target law-abiding citizens or infringe on speech, religion, assembly, or due process rights. This challenge highlights how government counterterrorism work in the secretive operational realm depicted in **Figure 1** can influence engagement conducted in the open marketplace of ideas. If a community views government counterterrorism investigative activity as overly aggressive, it may not willingly cooperate in engagement programs. One expert has noted that "counter-radicalization is not about intelligence-gathering nor is it primarily about policing."⁵² The HSAC Countering Violent Extremism Working Group found that

There can be tension between those involved in law enforcement investigations and those collaborating to establish local partnerships to stop violent crime. Community policing can be impeded if other enforcement tactics are perceived as conflicting with community partnership efforts.⁵³

This challenge is evident in some public discussions of law enforcement surveillance activities and efforts to recruit and manage informants. Revelations that the NYPD engaged in surveillance of mosques, Muslim businesses, and Muslim college students in New Jersey and elsewhere in 2006 and 2007 have prompted concern among a number of community groups and civil libertarians.⁵⁴ The FBI's top official in New Jersey suggested that such activities undermined the bureau's efforts at community engagement.⁵⁵ While New York City Mayor Michael Bloomberg and others defended the legality of such activities, some New Jersey officials have complained that the NYPD had not effectively coordinated efforts with them.⁵⁶ Other former law enforcement officials in New Jersey believed that appropriate cooperation occurred.⁵⁷ Also, as announced in May 2012, a fact-finding review conducted by New Jersey's Office of the Attorney General "revealed no evidence ... that NYPD's activities in the state violated New Jersey civil or criminal laws."⁵⁸

In pursuing a community engagement strategy, the use of informants can be a controversial issue, especially when law enforcement officials rely on informants with criminal records who may be

⁵² Neumann, *Preventing Violent Radicalization*, p. 19.

⁵³ HSAC CVE Working Group, Spring 2010, p 6.

⁵⁴ Samantha Henry, "NJ Muslims, Officials Discuss NYPD Surveillance," *Associated Press*, March 3, 2012. Hereafter: Henry "NJ Muslims, Officials." Chris Hawley, "NYPD Monitored Muslim Students All Over Northeast," *Associated Press*, February 18, 2012.

⁵⁵ Samantha Henry, "NJ FBI Says NYPD Monitoring Damaged Muslims' Trust," *Associated Press*, March 8, 2012.

⁵⁶ Henry, "NJ Muslims, Officials;" Jason Grant, "Recent NYPD Spying Uproar Shakes FBI's Foundations in N.J. Terror Intelligence," *Star-Ledger*, March 7, 2012, http://www.nj.com/news/index.ssf/2012/03/recent_nypd_spying_uproar_shak.html.

⁵⁷ Christopher Baxter, "Secret NYPD Surveillance in N.J. Was Not So Secret, Former Officials Say," *Star-Ledger*, March 6, 2012, http://www.nj.com/news/index.ssf/2012/03/secret_nypd_surveillance_in_nj.html.

⁵⁸ New Jersey Office of the Attorney General, press release, "Office of the Attorney General Takes Steps to Address Out-of-State Law Enforcement Activity in New Jersey Following Fact-Finding Review," May 24, 2012, <http://www.nj.gov/oag/newsreleases12/pr20120524b.html>.

working on behalf of authorities in exchange for reduced jail time. One Muslim community leader who has published widely on domestic terrorism, states that “many Muslim Americans fear that paid FBI informants specifically target impressionable youth and that law enforcement agents coerce community members to become informants themselves to avoid complications with immigration procedures.”⁵⁹ Confidential informants have been used in post-9/11 violent jihadist cases occurring in the United States. In some of those cases, the informants had criminal histories. The use of informants poses the following risks:

Informants do not merely observe and collect data. They make things happen.... Informants can cause confusion and dissatisfaction among members of groups and communities they infiltrate, discrediting leaders, and fostering factionalism as people wonder if any of their colleagues are spies. Their handlers’ structure of incentives—raises, promotions, transfers, financial rewards, waived jail time—creates a system where informants consciously or subconsciously create and then destroy terrorist threats that would not otherwise exist. These pressures can push them from passive observer to aggressive actor, with serious consequences for constitutionally protected free speech. Another unplanned result: government loses legitimacy and support in the eyes of targeted communities, if they feel they have been manipulated.⁶⁰

Acknowledging the challenge, FBI Director Robert Mueller said in 2009, “Oftentimes, the communities from which we need the most help are those who trust us the least. But it is in these communities that we ... must redouble our efforts.”⁶¹ Also in 2009, then-FBI spokesman John Miller said the agency values its relationships with Muslims and has worked hard on outreach efforts that range from town hall meetings to diversity training for FBI agents.⁶² Miller said there

⁵⁹ Alejandro J. Beutel, “Muslim Americans and U.S. Law Enforcement: Not Enemies, But Vital Partners,” *The Christian Science Monitor*, December 30, 2009, <http://www.csmonitor.com/Commentary/Opinion/2009/1230/Muslim-Americans-and-US-law-enforcement-not-enemies-but-vital-partners>. For more information on controversies surrounding informants, see Peter Finn, “Documents Provide Rare Insight Into FBI’s Terrorism Stings,” *Washington Post*, April 13, 2012, http://www.washingtonpost.com/world/national-security/documents-provide-rare-insight-into-fbis-terrorism-stings/2012/04/13/g1QASJ6CGT_story.html; Jerry Markon, “Lawsuit Alleges FBI Violated Muslims’ Freedom of Religion,” *Washington Post*, February 22, 2011, <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/22/AR2011022206975.html>; Jerry Markon, “Mosque Infiltration Feeds Muslims’ Distrust of FBI,” *Washington Post*, December 5, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/04/AR2010120403720.html>; Salvador Hernandez, “Release Terms Eased for Man Accused of Lying About Alleged Terrorist Ties,” *The Orange County Register*, June 11, 2010, <http://www.ocregister.com/articles/niazi-252994-fbi-case.html?pic=1>; Trevor Aronson, “FBI Tries to Deport Muslim Man for Refusing to be an Informant,” *miaminewtimes.com*, Oct 8, 2009, <http://www.miaminewtimes.com/2009-10-08/news/unholy-war-fbi-tries-to-deport-north-miami-beach-imam-foad-farabi-for-refusing-to-be-an-informant/>; “FBI Creates Climate of Fear,” *Orange County Register*, Editorial, March 22, 2009, <http://www.ocregister.com/articles/fbi-18893-ocprint-fear-.html>; Teresa Watanabe and Paloma Esquivel, “L.A. Area Muslims Say FBI Surveillance Has a Chilling Effect on Their Free Speech and Religious Practices,” *Los Angeles Times*, March 1, 2009, <http://articles.latimes.com/2009/mar/01/local/me-muslim1>. Hereafter: Watanabe and Esquivel, March 1, 2009. Thomas Cincotta, “From Movements to Mosques, Informants Endanger Democracy,” *The Public Eye*, summer 2009, <http://www.publiceye.org/magazine/v24n2/movements-to-mosques.html>. Hereafter: Cincotta, “From Movements to Mosques.” Lee Romney, “Immigrant Says FBI Tried Threats to Make Him Spy,” *Los Angeles Times*, August 12, 2006; <http://www.chron.com/disp/story.mpl/front/4112103.html>. Peter Waldman, “A Muslim’s Choice: Turn U.S. Informant or Risk Losing Visa,” *Wall Street Journal*, July 11, 2006, <http://www.legalsanctuary.org/doc/article13970.pdf>.

⁶⁰ Cincotta, “From Movements to Mosques.”

⁶¹ Quoted in Matthai Kuruwila, “U.S. Muslims Debate How Much to Help FBI,” *San Francisco Chronicle*, April 6, 2009, http://articles.sfgate.com/2009-04-06/news/17193854_1_american-muslim-taskforce-muslim-community-american-islamic-relations.

⁶² Quoted in Samantha Henry, “Some Muslims Rethink Close Ties to Law Enforcement,” *Associated Press*, May 4, 2009, http://www.breitbart.com/article.php?id=D97VII09O0&show_article=1.

is no factual basis for claims the FBI infiltrates mosques or conducts blanket surveillance of Muslim leaders. “Based on information of a threat of violence or a crime, we investigate individuals, and those investigations may take us to the places those individuals go.”⁶³

Former FBI agents and federal prosecutors note that informants are “still one of the government’s best weapons to thwart terrorists and that the benefit to national security is likely to far outweigh any embarrassment to the agency.” They claim that “although the law places almost no constraints on the use of informants, the agency takes sending an informant into a mosque very seriously and imposes a higher threshold for such requests.”⁶⁴ Former FBI counterterrorism Chief Robert Blitzer, states that “What matters to the FBI is preventing a massive attack that might be planned by some people ... using the mosque or church as a shield because they believe they’re safe there. That is what the American people want the FBI to do. They don’t want some type of attack happening on U.S. soil because the FBI didn’t act on information.”⁶⁵

Maher Hathout from the Muslim Public Affairs Council counters by saying that “People cannot be suspects and partners at the same time. Unless the FBI’s style changes, the partnership with the Muslim community will not be fruitful.”⁶⁶ The HSAC’s CVE Working Group also cautions that “Law enforcement should be sensitive to the fact that perceptions regarding enforcement actions and intelligence gathering can impact community-oriented policing goals.”⁶⁷ In considering the tradeoff between security and liberty, policy makers face a choice in those cases where an investigative tactic might inflame members of a particular community: Is the impact of that tactic counterproductive in the long run, or is it necessary, short-term collateral damage?

U.S. Attorneys as Brokers

As mentioned elsewhere in this report, DOJ has pushed the U.S. Attorneys to become larger players in community outreach. This suggests a critical question: is it appropriate to have the nation’s principal litigators be key players in the federal government’s CVE outreach efforts? Can the same people responsible for prosecuting terrorism cases effectively broker trust among community members who may be wary of federal law enforcement? Maintaining the integrity of this dualistic U.S. Attorney role—chief terrorism litigators v. federal outreach coordinators—may be challenging in the implementation of the strategy.

Legitimacy and Litmus Tests

Given their role in federal CVE engagement, U.S. Attorneys have to selectively cooperate with groups at the local level. Identifying specific groups for outreach may be challenging. There is

⁶³ Ibid. In March 2012, the American Civil Liberties Union (ACLU) asserted that the FBI had used outreach efforts at mosques in California to gather intelligence. Much of the outreach activity critiqued by the ACLU occurred several years ago. FBI denied that the outreach was used to gather intelligence. See http://www.aclu.org/files/assets/aclu_eye_on_the_fbi_-_mosque_outreach_03272012_0.pdf; Dan Levine, “FBI Said to Have Gathered Intelligence on California Muslims,” *Reuters*, March 27, 2012, <http://www.reuters.com/article/2012/03/28/us-usa-california-muslims-idUSBRE82R00Y20120328>.

⁶⁴ Gillian Flaccus. “Calif. Case Highlights Use of Mosque Informants.” *Associated Press*, March 1 2009. http://www.breitbart.com/article.php?id=D96LD2A81&show_article=1.

⁶⁵ Ibid.

⁶⁶ Watanabe and Esquivel, March 1, 2009.

⁶⁷ HSAC CVE Working Group. Spring 2010, p. 6.

little consensus among American Muslims regarding national advocacy groups: “many Muslims do not feel there is a national Muslim-American organization that represents them. When asked which of a list of national Muslim-American organizations represents their interests, 55% of Muslim men and 42% of Muslim women say that none do.”⁶⁸

The U.S. government can affect the legitimacy of community actors simply by choosing them as outreach partners. It is unclear how U.S. Attorneys will select the groups with which they will work. To this end, will the U.S. government establish litmus tests regarding federal interaction with community groups? What role will law enforcement considerations—potentially choosing only groups that have cooperated with FBI investigations by offering leads or providing informants, for example—play in the selection of community partners? Will federal investigators scour the backgrounds of groups prior to engaging with them?

When selecting engagement partners, DOJ has made at least one very public choice that was driven by law enforcement or prosecutorial considerations. The FBI and DOJ have limited their ties to the Council on American-Islamic Relations (CAIR), because DOJ listed the group as an unindicted co-conspirator in a federal terrorism case.⁶⁹ This is an example of the dynamics described in **Figure 1**—the secretive (operational) realm driving community engagement activity in the marketplace of ideas. In November 2008, the Holy Land Foundation for Relief and Development and five of its leaders were convicted of providing material support to Hamas, a designated foreign terrorist organization.⁷⁰ CAIR has opposed its listing as an unindicted co-conspirator. The listing is not a formal criminal charge, and subsequent terrorism charges have not been brought against CAIR.⁷¹ In spite of all of this, CAIR, a well-known Muslim advocacy group, maintains working relationships with local law enforcement officials.⁷²

Fusion Centers and Community Engagement—Potentially Alleviating Tensions

The CVE strategy mentions the role of the national network of fusion centers⁷³ in alleviating tension between the government’s investigative and engagement activities. Fusion centers play a

⁶⁸ *Muslim Americans: Faith, Freedom, and the Future; Examining U.S. Muslims’ Political, Social, and Spiritual Engagement 10 Years After September 11*, Abu Dhabi Gallup Center, August 2011, p. 25, <http://www.abudhabigallupcenter.com/148778/REPORT-BILINGUAL-Muslim-Americans-Faith-Freedom-Future.aspx>. Hereafter: *Muslim Americans: Faith, Freedom, and the Future*.

⁶⁹ Letter from Richard C. Powers, FBI Assistant Director, to U.S. Senator Jon Kyl, April 28, 2009.

⁷⁰ Transcript of Hearing, “Rep. Frank R. Wolf Holds a Hearing on Justice Department Budget,” *Political Transcript Wire*, March 1, 2012; DOJ, press release, “Federal Judge Hands Downs Sentences in Holy Land Foundation Case,” May 27, 2009, <http://www.justice.gov/opa/pr/2009/May/09-nsd-519.html>. For more on CAIR’s origins and relationship with the U.S. government, see Lorenzo Vidino, *The New Muslim Brotherhood in the West* (New York: Columbia University Press, 2010), pp. 177-197. In the fall of 2008, the FBI limited its interactions with CAIR.

⁷¹ CAIR, press release, “Top Internet Disinformation About CAIR,” http://www.cair.com/Portals/0/pdf/Dispelling_Rumors_about_CAIR.pdf.

⁷² Scott Shane, “Congressional Hearing Puts Muslim Civil Rights Group in the Hot Seat Again,” *New York Times*, March 11, 2011, <http://www.nytimes.com/2011/03/12/us/politics/12muslims.html?scp=3&sq=&st=nyt>.

⁷³ DHS recognizes a national network of state and local intelligence fusion centers. The network consists of centers that function as “collaborative effort[s] of two or more agencies that provide resources, expertise, and information ... with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.” See *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, August 2006, p. 12, http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf. For a list of fusion centers, see Department of Homeland Security, “Fusion Center Locations and Contact Information,” February 22, 2012, http://www.dhs.gov/files/programs/gc_1301685827335.shtm.

part in reporting suspicious, terrorism-related activity nationwide, perhaps potentially causing some tension between communities and law enforcement.⁷⁴ The strategy and the SIP mention the Building Communities of Trust Initiative (BCOT) as a project fostering relationships among three sets of actors—fusion centers, law enforcement, and the communities in which they operate.⁷⁵ This type of outreach potentially informs local communities about how suspicious activity suggestive of terrorism is reported to law enforcement and how police protect civil rights and liberties as they look for such activity.⁷⁶ The initiative’s recommendations included items such as

- training of fusion center analysts in cultural sensitivity so that they can distinguish behavior that is constitutionally protected from criminal or terrorist activity;
- encouraging law enforcement to “embrace” community policing by “emphasizing partnerships and problem solving”; and
- encouraging communities to view information sharing with fusion centers and law enforcement as key to crime prevention and counterterrorism.⁷⁷

Building Government and Law Enforcement Expertise

The SIP emphasizes three key items in this area. First, the plan notes that the U.S. government has to improve its understanding of radicalization via research, analysis, and partnerships. Second, greater sharing of information among state, local, and federal agencies regarding terrorist recruitment and radicalization is necessary.⁷⁸ Third, the SIP notes that the federal government has to improve the radicalization-related training offered to federal, state, and local agencies.

Paramount among the federal government’s efforts to improve its understanding of CVE are efforts to study the radicalization process and identify radicalizing individuals. To this end, as of March 2012, the National Institute of Justice included research on domestic radicalization in its preliminary list of forthcoming funding opportunities.⁷⁹ The Science and Technology Directorate (S&T) within DHS has also pursued the topic. The Department claims that since 2009, S&T has developed more than 20 reports in this area.⁸⁰ To help identify radicalizing individuals, DHS, the FBI, and the National Counterterrorism Center (NCTC) produced a study of homegrown terrorists, which reportedly teased out warning signs of radicalization. The study was discussed by senior federal, state, and local law enforcement officials at the White House in January 2012.⁸¹ Along these same lines, in July 2011, NCTC released findings resulting from an interagency study of homegrown terrorists. This study was not made public officially, but a summary of its findings is available online. It describes four “mobilizing patterns” among extremists. These include “links to known extremists, ideological commitment to extremism, international travel,

⁷⁴ For more on suspicious activity reporting see CRS Report R40901, *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress*, by Jerome P. Bjelopera.

⁷⁵ See Robert Wasserman, *Guidance for Building Communities of Trust*, July 2010, pp. 4-5, http://nsi.ncirc.gov/documents/c071021293_BuildingCommTrust_v2-August%2016.pdf. Hereafter: Wasserman, *Guidance for Building*.

⁷⁶ *Strategic Implementation Plan*, p. 9.

⁷⁷ Wasserman, *Guidance for Building*, pp. 4-5.

⁷⁸ *Strategic Implementation Plan*, pp. 12-18.

⁷⁹ See <http://www.nij.gov/nij/funding/forthcoming.htm>. For the Congressional appropriation see P.L. 112-55, p. 615.

⁸⁰ DHS, Fact Sheet, p. 2.

⁸¹ Eileen Sullivan, “Police Chiefs Meet at WH on Homegrown Terror Fight,” *Associated Press*, January 18, 2012.

and pursuit of weapons and associated training.”⁸² It also emphasized an approach to understanding and assessing radicalization via analysis of behavioral indicators.⁸³

The SIP also calls for enhanced information sharing between federal, state, and local law enforcement. Prior to late 2011, these efforts largely revolved around disseminating information to and briefing state and local officials. Such activity included the development of case studies examining the experiences of known and suspected terrorists.⁸⁴ This was recommended in 2010 by the HSAC.⁸⁵ In February 2011 congressional testimony, DHS Secretary, Janet Napolitano remarked that DHS develops these *unclassified* case studies so

that state and local law enforcement, state and local governments, and community members can understand the warning signs that could indicate a developing terrorist attack. These case studies focus on common behaviors and indicators regarding violent extremism to increase overall situational awareness and provide law enforcement with information on tactics, techniques, and plans of international and domestic terrorists.⁸⁶

Napolitano went on to note that DHS conducted what she dubbed “deep dive sessions” regarding CVE issues with local police intelligence experts—providing them with information they could pass to subordinates.⁸⁷

Additionally, the SIP notes that the federal government will enhance the radicalization-related training offered to federal, state, and local agencies. It argues that this is necessary because of “a small number of instances of federally sponsored or funded CVE-related and counterterrorism training that used offensive and inaccurate information.”⁸⁸ In March 2011, news reports and a study suggested that state and local law enforcement officials were receiving poor counterterrorism training from unqualified instructors, often from the private sector.⁸⁹ Furthermore, news reports indicated that offensive material produced by an FBI employee was delivered in a variety of official training sessions up until August 2011.⁹⁰ These revelations led to concerns from public officials and advocacy groups regarding training standards used by the bureau.⁹¹ In addition, reportedly biased material had seeped into the training made available to Joint Terrorism Task Force⁹² officers via a secure computer network.⁹³

⁸² National Counterterrorism Center, “Behavioral Indicators Offer Insights for Spotting Extremists Mobilizing for Violence, July 22, 2011, p. 1.

⁸³ *Ibid.*

⁸⁴ *Strategic Implementation Plan*, p. 14.

⁸⁵ HSAC CVE Working Group, Spring 2010, p. 20.

⁸⁶ U.S. Congress, House of Representatives Committee on Homeland Security, Written Testimony of Janet Napolitano, Secretary of the Department of Homeland Security, “Understanding the Homeland Threat Landscape –Considerations for the 112th Congress,” 112th Cong., 1st sess., February 9, 2011, p. 5.

⁸⁷ *Ibid.*

⁸⁸ *Strategic Implementation Plan*, p. 15.

⁸⁹ Dina Temple-Raston, “New Concern About Bias In Counterterror Training,” *National Public Radio*, March 9, 2011, <http://www.npr.org/2011/03/09/134374232/new-concern-about-bias-in-counterterror-training?ps-rs>; Thomas Cincotta, *Manufacturing the Muslim Menace: Private Firms, Public Servants, and the Threat to Rights and Security*, 2011, Public Research Associates, http://www.publiceye.org/liberty/training/Muslim_Menace_Complete.pdf.

⁹⁰ Spencer Ackerman and Noah Shachtman, “Video: FBI Trainer Says Forget ‘Irrelevant’ al-Qaida, Target Islam,” *Wired*, September 20, 2011, <http://www.wired.com/dangerroom/2011/09/fbi-islam-qaida-irrelevant/all/1>.

⁹¹ Letter from Sen. Joseph I. Lieberman and Sen. Susan M. Collins, to Eric H. Holder, Jr., Attorney General, and Janet Napolitano, Secretary of Homeland Security, March 29, 2011, <http://www.hsgac.senate.gov/reports/letters>. For an (continued...)

In the midst of these revelations, in September 2011 the bureau announced a review

of all training and reference materials that relate in any way to religion or culture. Additionally, the FBI will consult with outside experts on the development and use of training materials to best ensure the highest level of quality for new agent training, continuing education for all employees, and any FBI-affiliated training. All training will be consistent with FBI core values, the highest professional standards, and adherence to the Constitution.⁹⁴

DOJ announced a similar review in September 2011 as well.⁹⁵ Less than one percent of the material inspected was found to be inaccurate or inappropriate.⁹⁶ In October 2011, the White House ordered a broader examination of CVE instructional efforts within the federal government.⁹⁷ In the same month, DHS released guidance and best practices for CVE training. These highlighted five commonsense goals:

1. Trainers and training should be expert and well-regarded.
2. Training should be sensitive to constitutional values.
3. Training should facilitate further dialog and learning.
4. Training should adhere to government standards and efforts.
5. Training and objectives should be appropriately tailored, focused, and supported.⁹⁸

(...continued)

example of concerns voiced by advocacy groups see Letter from American Civil Liberties Union et al., to Robert S. Mueller, III, Director, Federal Bureau of Investigation, October 4, 2011, http://www.aclu.org/files/assets/sign_on_letter_to_dir_mueller_re_radicalization_report_10.4.11.pdf. Some Members of Congress also wrote to Attorney General Eric H. Holder, Jr. and Secretary of Defense, Leon E. Panetta regarding potential censorship of training material after the fallout surrounding the FBI's training efforts. See Letter from Rep. Sue Myrick et al. to Eric H. Holder, Jr., Attorney General, and Leon E. Panetta, Secretary of Defense, December 15, 2011, http://myrick.house.gov/uploads/12152011_Letter%20to%20DOJ%20and%20DOD%20re%20CT%20training%20changes.pdf.

⁹² Joint Terrorism Task Forces (JTTFs) are locally based, multi-agency teams of investigators, analysts, linguists, SWAT experts, and other specialists who investigate terrorism and terrorism-related crimes. Seventy-one of the more than 100 JTTFs currently operated by DOJ and the FBI were created since 9/11. Over 4,400 federal, state, and local law enforcement officers and agents more than four times the pre-9/11 total work in them. These officers and agents come from more than 600 state and local agencies and 50 federal agencies. See Federal Bureau of Investigation, "Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces," http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jtffs.

⁹³ Spencer Ackerman, "Obama Orders Government to Clean Up Terror Training," *Wired*, November 29, 2011, <http://www.wired.com/dangerroom/2011/11/obama-islamophobia-review/>. Hereafter: Ackerman, "Obama Orders."

⁹⁴ FBI, press release, "FBI Launches Comprehensive Review of Training Program," September 20, 2011, <http://www.fbi.gov/news/pressrel/press-releases/fbi-launches-comprehensive-review-of-training-program>.

⁹⁵ James M. Cole, Deputy Attorney General, memorandum for heads of DOJ components and United States Attorneys, "Training Guiding Principles," March 20, 2012, <http://www.justice.gov/dag/training-guiding-principles.pdf>. Hereafter, Cole, memorandum.

⁹⁶ Letter from Greg Fowler, Special Agent in Charge, FBI Portland Division, to Community Partners, March 28, 2012, http://www.fbi.gov/portland/news-and-outreach/stories/letter-to-community-partners?utm_campaign=email-Immediate&utm_medium=email&utm_source=portland-top-stories&utm_content=83167.

⁹⁷ Ackerman, "Obama Orders."

⁹⁸ CRCL, *Countering Violent Extremism (CVE) Training Guidance and Best Practices*, 2011, <http://training.fcma.gov/> (continued...)

The same document notes that CVE education programs differ from strictly counterterrorism training (the latter presumably centered on topics such as terrorist threats, vulnerabilities, and trends in terrorism). CVE training focuses “on developing trust, enhancing community resiliency, prevention, intervention, and protecting civil rights and civil liberties.”⁹⁹ In March 2012, DOJ and FBI released their own sets of training principles that parallel DHS’s goals.¹⁰⁰

Risks and Challenges

Development of better training and improved information sharing are laudable law enforcement goals. However, because such efforts feature so prominently in the second SIP objective, its overall thrust may be perceived to be more about classic preventative policing than about countering radicalization at the grass-roots level. It is unclear how much of the activity described under this objective directly fits into the Administration’s emphasis on “a community based” CVE approach.¹⁰¹

There is space in the CVE strategy for training law enforcement about constitutionally protected aspects of the radicalization process—in other words, efforts to train police to understand when suspects go from being law-abiding radicals to being terrorists. However, the SIP itself does not offer any formal means for federal, state, or local law enforcement to cope with radicalizing individuals outside of their traditional areas of expertise—investigation, arrest, and prosecution. The SIP does not outline mechanisms for law enforcement to refer radicalizing individuals for community intervention (whatever that might mean within a local context). Without such a process, police can become very adept at identifying radicalization and yet be only able to cope with a radicalized individual when he or she mobilizes and becomes a terrorism suspect. One of the risks implicit in this SIP objective is that it may sharpen police ability to investigate terrorists, without improving their ability to intervene with radicalizing individuals.

If the SIP’s efforts to improve law enforcement training mostly enhance the ability of police to detain suspects and provide no other means for coping with radicalization, then these elements of the strategy might be better described as counterterrorism in nature, not part of the nation’s counter-radicalization strategy.

The Issue of Openness

Should the federal government be concerned about the over-classification of radicalization-related research and training material by the security agencies involved in its development? The SIP’s second objective is an area in which a great deal of activity can occur behind closed doors

(...continued)

EMIWeb/docs/shared/CVE.%20Training%20Guidance.pdf. Hereafter: CRCL, *Training Guidance*. The Federal Emergency Management Agency (FEMA) also issued a bulletin regarding the same issues. FEMA grants can be used for CVE training. See FEMA, *Grant Programs Directorate Information Bulletin*, October 7, 2011, <http://www.fema.gov/pdf/government/grant/bulletins/info373.pdf>.

⁹⁹ CRCL, *Training Guidance*. DHS defines “resiliency” as the “ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions.” See; HSAC, *Community Resiliency Task Force Recommendations*, June 2011, p. 8, <http://www.dhs.gov/xlibrary/assets/hsac-community-resiliency-task-force-recommendations-072011.pdf>.

¹⁰⁰ Cole, memorandum; FBI, *The FBI’s Guiding Principles: Touchstone Document on Training 2012*, March 2012, <http://www.fbi.gov/about-us/training/the-fbis-guiding-principles>.

¹⁰¹ *Empowering Local Partners*, p. 2.

(within the secretive realm described in **Figure 1**), especially if the objective largely involves security, intelligence, and law enforcement agencies that typically avoid public disclosure of much of their other work. *However*, the steps involved in the radicalization process involve largely constitutionally-protected activity that occurs in the public sphere. Excessive secretiveness regarding government efforts to understand the legally protected activities of Americans might actually fuel radicalization. For example, one study by a British think tank has suggested that conspiracy theories “are a reaction to the lack of transparency and openness in many of our [U.K.] institutions.” This same study sees conspiracies as a “radicalizing multiplier.”¹⁰² Could this be possible in the United States?

A project developed as part of the second SIP objective was not widely released. The study of radicalization among homegrown violent extremists performed by DHS, NCTC, and the FBI—mentioned above—was revealed to state and local law enforcement behind closed doors at the White House. This example poses the question: can the federal government build trust within local communities if it holds back from the general public its own study of how people in the United States radicalized and became terrorists? Will secretiveness in this area actually feed radical narratives?

Additionally, will excessively secret government efforts to understand radicalization shake community trust in law enforcement? Federal attempts to develop *classified* theories about legally-protected activities may make community groups less willing to “share” information regarding those very activities—*especially if that information is treated strictly as intelligence by the government and the results of such “sharing” are never seen*. Transparency in this arena potentially opens government conceptualizations of radicalization and federal training materials to the scrutiny of outside experts. It is unclear what sway partnerships with non-government experts will have in the SIP’s second objective.

Talking about Ideology

Ideology is a key ingredient in the radicalization experience. It is unclear how the CVE Training Guidance issued by DHS accommodates discussion of ideology within an instructional environment. In fact, under one of its goals: “Training should be sensitive to constitutional values,” the guidance indicates that “Training should focus on behavior, not appearance or membership in particular ethnic or religious communities,” yet it is silent regarding radical ideologies. Should instructors focus on ideology? How should instructors discuss radical beliefs in the classroom?

Countering Violent Extremist Propaganda

The SIP notes that countering violent extremist propaganda is “the most challenging area of work, requiring careful consideration of a number of legal issues, especially those related to the First Amendment.”¹⁰³ In this area the document highlights NCTC’s efforts to develop a “Community Awareness Briefing.” In 2010, NCTC’s Director described the briefing in testimony to the Senate Homeland Security and Governmental Affairs Committee:

¹⁰² Jamie Bartlett and Carl Miller, *The Power of Unreason: Conspiracy Theories, Extremism, and Counter-Terrorism*, Demos, London, August 29, 2010, pp. 21, 39.

¹⁰³ *Ibid.*, p. 18.

It has become clear that government can play a significant role by acting as a convener and facilitator that informs and supports—but does not direct—community-led initiatives. Based on this, NCTC led the development of a Community Awareness Briefing that conveys unclassified information about the realities of terrorist recruitment in the Homeland and on the Internet. The briefing, which can be used by departments and agencies and has garnered very positive reactions, aims to educate and empower parents and community leaders to combat violent extremist narratives and recruitment.¹⁰⁴

NCTC has also connected community activists with technology experts in a seminar to “maximize the use of technology to counter violent extremism online” and the Department of State has developed exchanges between foreign CVE experts and U.S. communities.¹⁰⁵ The SIP did not indicate any additional “current activity” in late 2011 to counter violent extremist propaganda other than working to inform the media, policy makers and U.S. communities on the issue. It does mention the development of a separate strategy for the digital environment.¹⁰⁶

Risks and Challenges

The SIP notes that government efforts to counter narratives that foster radicalization should affirm American unity and bolster community capacities to “contest violent extremist ideas.” The document stresses the importance of First Amendment concerns in this area.¹⁰⁷

Aside from First Amendment issues, a challenge in this area might revolve around the perceived legitimacy of the main agencies the Administration selects for its implementation efforts. If security agencies trawling the internet for potential suspects lead the charge in fostering a counter-narrative, will American Muslims see these efforts as legitimate?¹⁰⁸ How willing will they be to partner with FBI, DOJ, NCTC, and DHS to further this SIP goal?

One area in which these agencies may be able to leverage their reputations as part of the U.S. counterterrorism apparatus, build rapport within communities, and possibly forward efforts to counter extremist propaganda, involves personal online security. They can provide training regarding safe Internet navigation, how to avoid criminals online as well as websites sponsored by officially listed foreign terrorist organizations. They can talk to communities about what types of online activities prosecuted terrorists pursued, especially those activities documented in court proceedings and government press releases.

Administration Plan and Future Activities

The SIP lists “future activities and efforts” under its three objectives. **Figure 2**, **Figure 3**, and **Figure 4** each cover a single SIP objective. They depict the lead federal agencies responsible for

¹⁰⁴ Written Statement of Michael Leiter; Director, National Counterterrorism Center; U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland*, 111th Cong., 2nd sess., September 22, 2010, p. 8.

¹⁰⁵ *Strategic Implementation Plan*, p. 19.

¹⁰⁶ *Ibid.*, p. 20.

¹⁰⁷ *Ibid.*, p. 18.

¹⁰⁸ See CRS Report R42406, *Congressional Oversight of Agency Public Communications: Implications of Agency New Media Use*, by Kevin R. Kosar, for information regarding Congress’s role in oversight of federal public communications activities.

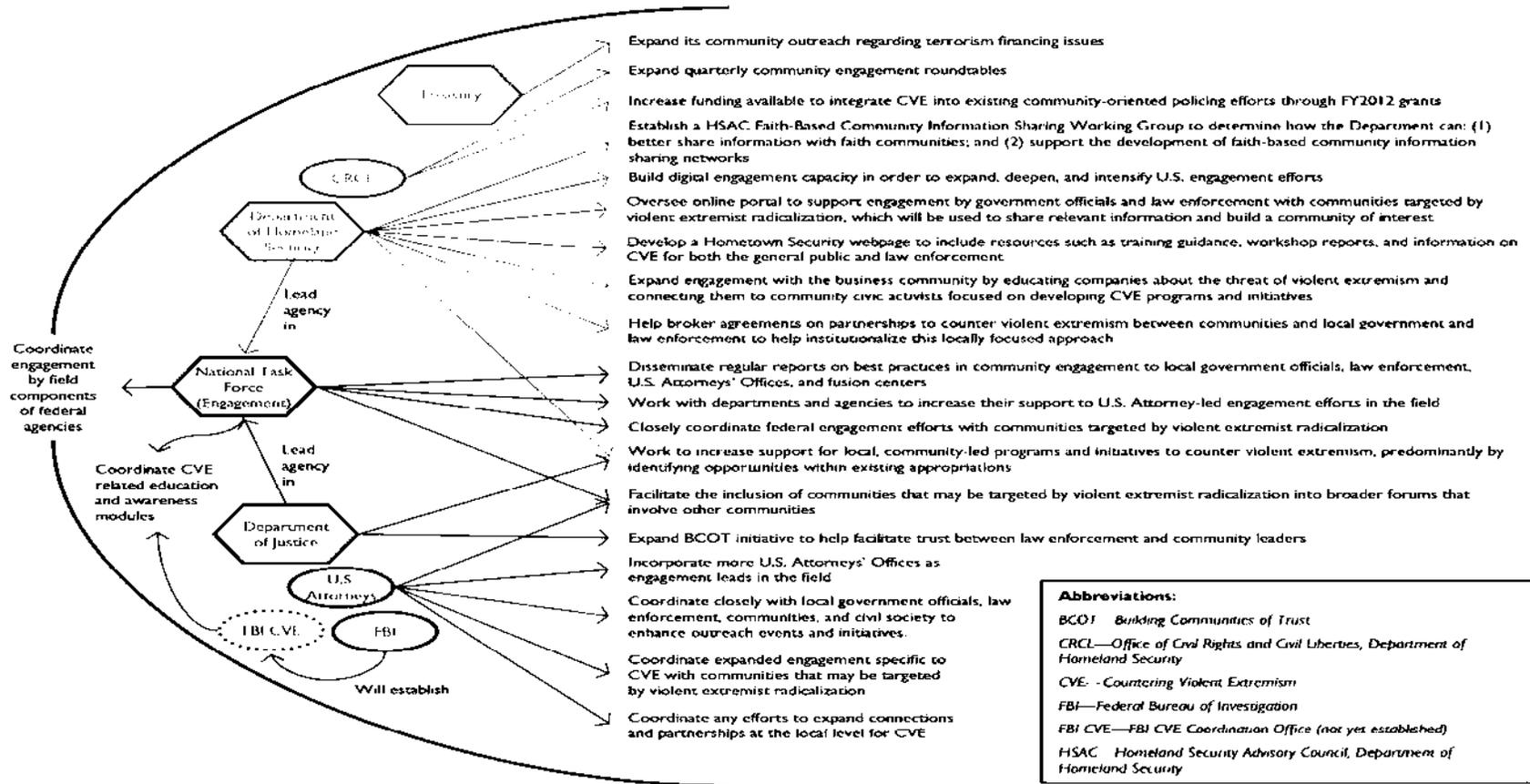
the future activities and efforts subsumed by the relevant objective, and more than one agency can serve as a lead for a particular effort. For the sake of clarity, the figures do not depict partner agencies playing secondary roles and assisting the lead agencies in particular activities. The language used for each of the future activities and efforts in the three figures extensively paraphrases or directly quotes the language used in the SIP. Additionally, the three figures do not include all of the component agencies of specific executive departments. Only the component agencies responsible for future activities and efforts under each SIP objective are included.

Is DHS the De Facto U.S. CVE Lead Agency?

It appears that DHS is cited as a lead agency in 43 of the 62 future activities and efforts discussed in the SIP.¹⁰⁹ Because it is a key player and decision maker in more than two-thirds of the SIP's impending plans, it seems that DHS may be the de facto lead agency in charge of U.S. CVE activity in the near future. This suggests a critical issue: while granted a large amount of responsibility for implementation of the CVE strategy, will DHS have a matching level of say in its further evolution?

¹⁰⁹ This count includes four responsibilities given to the National Task Force for engagement under the SIP. Both DHS and DOJ are lead agencies in the task force.

Figure 2. Lead Agencies and Their “Future Activities and Efforts” for SIP Objective I, Enhancing Federal Engagement and Support to Local Communities that may be Targeted by Violent Extremists

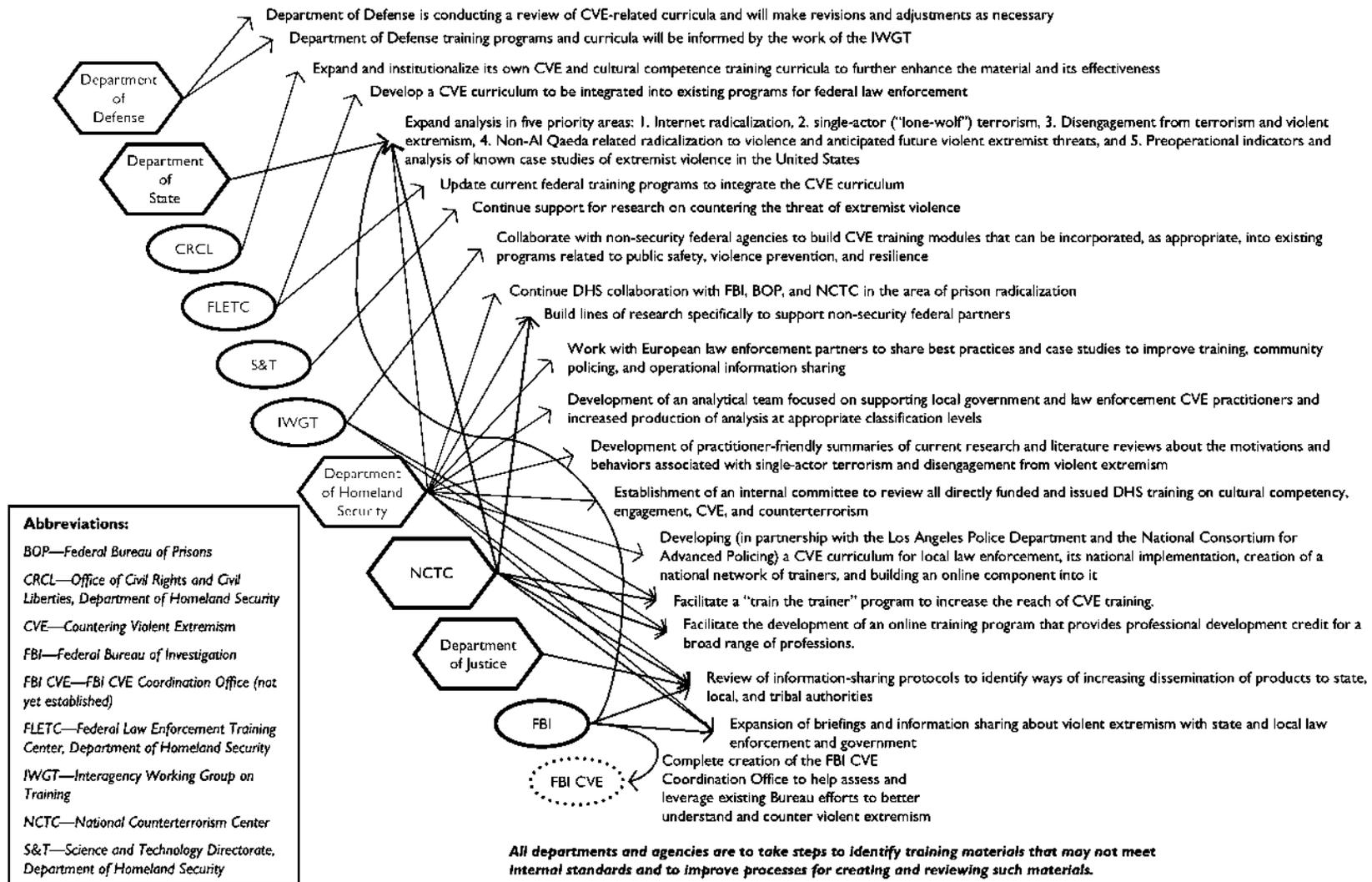


Key for SIP Future Activities Figures

Colors		Shapes
 Department of Defense	 National Counterterrorism Center	 Independent federal department or agency
 Department of Homeland Security	 National Task Force (Engagement)	 Component agency or office
 Department of Justice	 Treasury	 Future office
 Department of State		 Designated as lead agency for

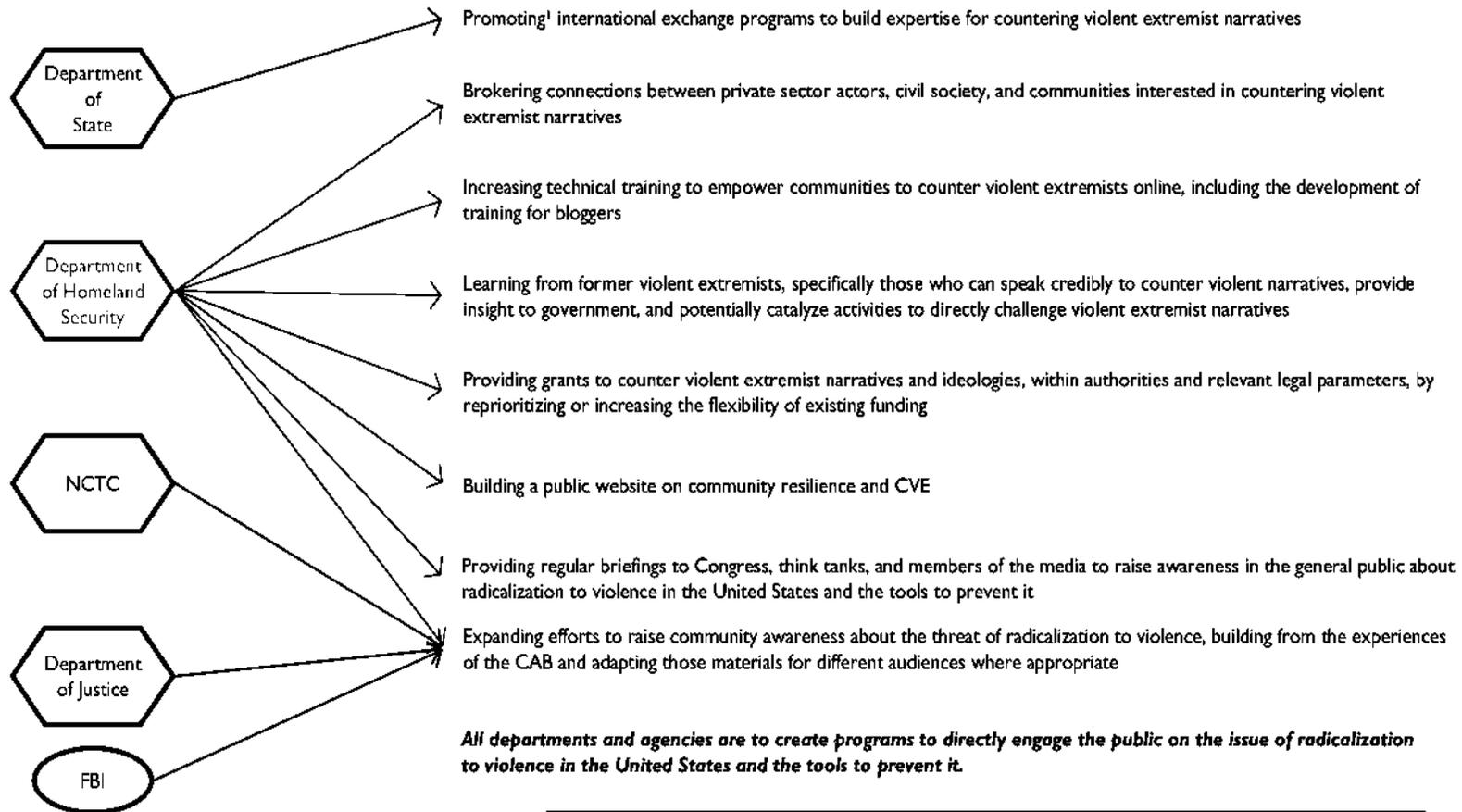
Source: CRS, based on materials contained in the SIP.

Figure 3. Lead Agencies and Their “Future Activities and Efforts” for SIP Objective 2, Building Government and Law Enforcement Expertise for Preventing Violent Extremism



Source: CRS, based on materials contained in the SIP.

Figure 4. Lead Agencies and Their “Future Activities and Efforts” for SIP Objective 3, Countering Violent Extremist Propaganda While Promoting U.S. Ideals



Abbreviations:	
CVE—Countering Violent Extremism	NCTC—National Counterterrorism Center
FBI—Federal Bureau of Investigation	CAB—Community Awareness Briefing, developed in 2010 by NCTC

Source: CRS, based on materials contained in the SIP.

Notes: The text in Figure 4 shifts to the present progressive tense, as does the text in the SIP related to the future activities and efforts for Objective 3.

Possible Policy Considerations for Congress

“The United States has made great strides,” says one federal counterterrorism official, “in what might be called tactical counterterrorism—taking individual terrorists off the streets, and disrupting cells and their operations ... an effective counterterrorism strategy must go beyond this ... (to address) the threat of violent extremism.”¹¹⁰ With the announcement of the CVE strategy, the Obama Administration has begun to address this concern. These Administration efforts may attract greater oversight from Congress, especially because the strategy involves the interplay between the public marketplace of ideas involving constitutionally-protected activity and the secretive operational realm where terrorists plot and law enforcement pursues.

Implementing the CVE Strategy

As mentioned elsewhere in this report, federal CVE activity emphasizes engagement with Muslim communities across the country. It broadly recognizes this, training, and counter messaging as key components of CVE. However, aside from embracing robust outreach and training for government agencies, the strategy lacks specific initiatives to combat radicalization at the grass-roots level. This suggests a number of other issues.

Picking Partners and Establishing “Rules of the Road”

Who speaks for diverse Muslim communities in America? As mentioned above, “[w]hen asked “which of a list of national Muslim-American organizations represents their interests, 55% of Muslim men and 42% of Muslim women say that none do.”¹¹¹ Perhaps sentiments are clearer at the local level, however these figures suggests the difficulty of selecting partners who accurately represent community needs. It is difficult to speak of one Muslim “constituency” in the United States. The 2.75 million Muslims in the United States have divergent sectarian points of view, come from many ethnic or national backgrounds, and live in a variety of areas. Muslim Americans support many secular and religious organizations.¹¹²

What criteria will the Administration employ in its selection efforts, and how transparent will the process be? Once approved as partners, what “rules of the road” will govern continued cooperation? In essence, what would have to happen for a Muslim community group to fall out of favor with the government? Ad hoc decision making might cause the whole CVE outreach process to appear arbitrary to some community participants. Congress may consider requiring the Administration to release public guidelines in this area. Public guidelines may be especially important, because engagement directly involves engaging people and issues in the open marketplace of ideas and protected constitutional activity.

¹¹⁰ Robert F. Godec, Principal Deputy Director for Counterterrorism at the Department of State, “U.S. Counterterrorism Policy,” an address before the Global Young Leaders Conference, Washington, DC; June 30, 2010, <http://www.state.gov/s/ct/rls/rm/2010/143809.htm>.

¹¹¹ *Muslim Americans: Faith, Freedom, and the Future*, p. 25.

¹¹² Qamar-ul Huda, *The Diversity of Muslims in the United States: Views as Americans*, United States Institute of Peace, Special Report 159, Washington, DC. February 2006. <http://www.usip.org/files/resources/sr159.pdf>. See also: Pew Research Center, *Muslim Americans: No Signs of Growth in Alienation or Support for Extremism*, August 2011, pp. 13-21, <http://www.people-press.org/files/legacy-pdf/Muslim-American-Report.pdf>.

Intervention with At-Risk Individuals

There appears to be little federally driven guidance to community groups on how to intervene with people vulnerable to radicalization.¹¹³ Such an intervention effort, the Channel Program, has been a key element of the United Kingdom’s counter radicalization strategy since 2007. The British government describes Channel as a “multi-agency programme to identify and provide support to people at risk of radicalisation” and involvement in “all forms of terrorism.”¹¹⁴ Channel “relies on close collaboration between police, partners and other key stakeholders ... and where necessary, provides an appropriate support package tailored to an individual’s needs.”¹¹⁵ Copying the Channel program in its entirety may not be appropriate for the U.S. context. However, it is unclear whether the Obama Administration considers some variant of Channel workable or even necessary in the United States.

The U.S. CVE strategy does cite the Office of Juvenile Justice and Delinquency Prevention (OJJDP) Comprehensive Gang Model as an example of “locally-based initiatives that connect communities and government to address community challenges through collaboration and the development of stakeholder networks.”¹¹⁶ OJJDP—a component of DOJ’s Office of Justice Programs—describes the model as “one of the few approaches to gangs that encompasses a multidisciplinary response to gangs on multiple levels.”¹¹⁷ The preventative model is intended as a blueprint for organizing local counter-gang efforts that do not necessarily result in law enforcement-driven outcomes, such as investigations, arrests, and prosecutions. For intervention, it targets young adult and teen gang members, not entities such as hate groups, prison gangs, or ideologically driven gangs consisting of adults.¹¹⁸ The model involves five strategies:

Community Mobilization: Involvement of local citizens, including former gang members and community groups and agencies, and the coordination of programs and staff functions within and across agencies.

Opportunities Provision: The development of a variety of specific education, training, and employment programs targeting gang-involved youth.

Social Intervention: Youth-serving agencies, schools, street outreach workers, grassroots groups, faith-based organizations, law enforcement agencies, and other criminal justice organizations reaching out and acting as links between gang-involved youth and their families, the conventional world, and needed services.

Suppression: Formal and informal social control procedures, including close supervision or monitoring of gang youth by agencies of the criminal justice system and also by community-based agencies, schools, and grassroots groups.

¹¹³ Aside from general mention in the *Strategic Implementation Plan*, p. 10.

¹¹⁴ *Prevent Strategy*, p. 54.

¹¹⁵ Association of Chief Police Officers, *National Channel Referral Figures*, <http://www.acpo.police.uk/ACPOBusinessAreas/PREVENT/NationalChannelReferralFigures.aspx>.

¹¹⁶ *Empowering Local Partners*, p. 4.

¹¹⁷ OJJDP, *OJJDP Comprehensive Gang Model: Planning for Implementation*, May 2009, p. 2. Hereafter: OJJDP, *Comprehensive Gang Model*.

¹¹⁸ OJJDP, *Comprehensive Gang Model*, p. 6.

Organizational Change and Development: Development and implementation of policies and procedures that result in the most effective use of available and potential resources to better address the gang problem.¹¹⁹

The model is designed to focus on youth active in gangs or those who exhibit factors indicating potential gang involvement. It also advocates engagement with the families of such youth. Among its many suggestions, the model discusses interventions such as job training, employment, family counseling, academic tutoring, and anger management classes for young people at-risk. It also calls on law enforcement agencies and courts to move beyond traditional roles in the suppression of gangs—urging them to consider more intervention-oriented activities such as referring youth to social service programs.¹²⁰

The CVE strategy provides little detail about how the Comprehensive Gang Model may be applied to keep vulnerable people from radicalizing and becoming terrorists. Congress may consider examining the utility and feasibility of developing a CVE intervention model for the United States. While elaborating the specific details of such a program may be best left to the federal agencies potentially involved, broadly and publicly exploring what shape it would take might be of value to Congress. Key questions may involve issues such as 1) which agencies would take the lead in creating a program based on the Comprehensive Gang Model? 2) how would the FBI have to adapt its counterterrorism mission—strictly focused on investigating and disrupting terrorist activity—to handle the notion of “social intervention” as suggested by the Comprehensive Gang Model?

Identifying Programs and Federal Contacts to Assist Grassroots CVE Efforts

The Administration’s CVE strategy stresses that “The best defenses against violent extremist ideologies are well-informed and equipped families, local communities, and local institutions.”¹²¹ Determining and explaining how local entities—whether public or private—should interact with federal partners may pose quite a challenge. For example, are there existing federal grant programs that can be harnessed by local actors to develop a CVE intervention program? A publicly available comprehensive list of grant programs that can be harnessed for CVE activities does not exist. Congress may opt to consider the feasibility or the value of such a list or a clearinghouse available to local entities to identify such programs. By possibly pursuing this, Congress may help to ensure that local constituents have better information about and more direct access to federal CVE programs. On the other hand, such a list may be perceived as an additional layer of bureaucracy between constituents and grant programs.

Countering Extremist Ideas: Choosing Good vs. Bad

As the United Kingdom has clearly stated in its counter-radicalization program, extremist ideologies play a role in radicalization.¹²² Furthermore, the National Security Council’s Quintan

¹¹⁹ National Gang Center, “About the OJJDP Comprehensive Gang Model,” <http://www.nationalgangcenter.gov/Comprehensive-Gang-Model/About>. “Suppression” was not emphasized in the Obama Administration’s national CVE strategy’s description of the Comprehensive Gang Model. The other components of the model were mentioned. See *Empowering Local Partners*, p. 4.

¹²⁰ OJJDP, *Comprehensive Gang Model*, p. 6.

¹²¹ *Empowering Local Partners*, p. 2.

¹²² *Prevent Strategy*, p. 7.

Wiktorowicz has commented that “We [the United States] will push back against the full scope of different violent ideologies with an inclusive, positive narrative.”¹²³ However, in the United States, mere belief in radical notions, no matter how reprehensible they are, is not necessarily illegal. The American Civil Liberties Union’s (ACLU) Michael German has stated that the ACLU is “deeply concerned about the potential for government censorship of Internet content based on the [CVE] strategy’s proposal for countering violent extremist propaganda.”¹²⁴

Even more fundamentally, the task of countering extremist ideas raises key issues regarding the implementation of the CVE strategy. In the SIP, the Administration notes that when countering violent extremist propaganda, “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.”¹²⁵ This begs the question: do the strategy and the SIP place the federal government in the business of determining which ideologies are dangerous and which are safe—essentially determining which beliefs are good and which are bad? This can be viewed from two angles. One involves establishing parameters for engagement with local communities, the other involves evaluating the end product of engagement, the counter-narrative.

- First, while the SIP may suggest that the government *should not* be involved in *creating* alternatives to violent extremist propaganda, it appears to assume that the government *will* be involved in *sifting* between dangerous and safe ideas—establishing parameters for engagement on this issue. Without picking and choosing between good and bad ideologies, “empowering” local activists to counter specific concepts may prove difficult. Empowering individuals and groups to counter un-named, un-described concepts may prove challenging.
- Second, if the framing of a counter-narrative challenging terrorist ideologies is necessary, how precisely should the federal government partner with state and local government and civilian counterparts in the development of this counter-narrative? How do government entities keep a counter-narrative from being publicly viewed as propaganda or fueling terrorist conspiracy theories about the United States?

Oversight in this area may be vital. As a start, Congress may wish to ask the Administration to better define what it means when referring to “violent extremist narratives.”

The Lack of a Lead Agency

There is no designated single lead agency for any of the three objectives laid out in the SIP. Likewise, there is no single agency managing all of the individual activities and efforts of the plan. At the national level, it arguably may be of value to have a single federal agency in charge of the government’s CVE efforts. One expert has stated as much:

¹²³ Dina Temple-Raston, “White House Unveils Counter-Extremism Plan,” *NPR*, August 3, 2011, <http://www.npr.org/2011/08/04/138955790/white-house-unveils-counter-extremism-plan>.

¹²⁴ “ACLU Lens: Obama Plan to Fight Violent Extremism a Step in the Right Direction, But...” *ACLU Blog of Rights*, August 3, 2011, <http://www.aclu.org/blog/national-security/aclu-lens-obama-plan-fight-violent-extremism-step-right-direction>.

¹²⁵ *Strategic Implementation Plan*, p. 18.

The White House should designate a single agency that serves as the principal hub for collecting, disseminating, and evaluating information on counter-radicalization. Its main function would be to collect, analyze, and share best practices with a wide range of governmental and non-governmental actors, including community leaders and non-profits.¹²⁶

Without a lead agency it may be difficult to monitor the levels of federal funding devoted to CVE efforts. How many personnel are devoted to CVE in the federal government? For how many of these employees is counter radicalization a full-time job? Are there mechanisms to track federal CVE expenditure? Which federal body is responsible for this? Very specifically, the lack of a lead agency is reflected in the fact that DOJ, DHS, and FBI have each issued training guidelines for CVE. They are very similar, but the issuance of three almost identical but separate guidelines raises the question: why not just have one set created by one body overseeing the CVE program? Congress may pursue with the Administration the feasibility or value of designating a lead agency, or the possibility of naming a lead via legislation. However, it is unclear what types of authority—especially in the budgetary realm—such a lead may be able to wield over well-established agencies playing central roles in the CVE strategy.

Measuring Input and Results

On the other side of these budgetary questions, without a lead agency, how will the Administration evaluate the effectiveness of federal CVE efforts? The SIP underscores that individual departments and agencies involved in CVE “will be responsible for assessing their specific activities in pursuit of SIP objectives, in coordination with an Assessment Working Group.”¹²⁷ While this may seem straight-forward, the British government has struggled with measurement issues related to its counter-radicalization strategy. U.K. officials have made “progress ... in measuring outputs but not always in measuring outcomes.”¹²⁸ In other words, counting the number of engagement events is one thing. It is quite another thing to evaluate their impact. The SIP mentions this problem as well.¹²⁹ However, the SIP does not discuss 1) specific metrics, 2) what real authority the Assessment Working Group will have to *independently* evaluate and impact CVE activity within federal departments and agencies, and 3) whether the Assessment Working Group will have the power to standardize measures of success across federal agencies and departments. In the end, the lack of a lead agency with budgetary control over CVE efforts and clear responsibility for implementation of the strategy makes it difficult to conceptualize exactly how spending in this area will be prioritized, evaluated, and then re-prioritized based on results.

Secretiveness vs. Transparency

Without a high degree of transparency, an engagement strategy driven by federal agencies charged with intelligence gathering and law enforcement responsibilities may run the risk of being perceived as an effort to co-opt communities into the security process—providing tips, leads, sources, and informants. This threatens to “securitize” a relationship intended as outreach within the marketplace of ideas. It has been noted that “unlike counterterrorism, which targets

¹²⁶ Neumann, *Preventing Violent Radicalization*, p. 41.

¹²⁷ *Strategic Implementation Plan*, p. 6.

¹²⁸ *Prevent Strategy*, p. 36.

¹²⁹ *Strategic Implementation Plan*, p. 6.

terrorists, counter-radicalization is focused on the communities that are targeted by terrorists for recruitment. The aim is to protect, strengthen, and empower these communities so that they become resilient to violent extremism.”¹³⁰ As such, some suggest that it might not be particularly effective to have the same federal agencies responsible for counterterrorism also be the main players in the CVE strategy.¹³¹ The SIP rejects this notion stressing that “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.”¹³² The strategy relies on agencies whose enforcement and intelligence missions are undergirded by secretiveness. As it stands, 19 of the 20 “future activities and efforts” for SIP objective 1, which focuses on community engagement, have DOJ, DHS, or a national task force headed by DOJ and DHS as lead agencies. The lone remaining future activity/effort is headed by the Department of Treasury and is focused on terrorism financing, an area of enforcement for the Department.

The fact that DOJ, DHS, and Treasury are key counterterrorism agencies may make it difficult for community groups to view them as full partners, especially if community confidence in them is shaky to start. According to a 2011 study, American Muslims have less confidence than other faith groups in the FBI—“60% of Muslim Americans saying they have confidence in the FBI, versus 75% or more of Americans of other faiths who say this.”¹³³ Because of this reality, Congress may decide to assess whether there is a need for greater transparency from the Administration in its CVE efforts.

Author Contact Information

Jerome P. Bjelopera
Specialist in Organized Crime and Terrorism
jbjelopera@crs.loc.gov, 7-0622

¹³⁰ Neumann, *Preventing Violent Radicalization*, p. 7.

¹³¹ *Ibid.*, p. 8.

¹³² *Strategic Implementation Plan*, p. 4.

¹³³ *Muslim Americans: Faith, Freedom, and the Future*, p. 23.

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

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

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

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

Countering Violent Extremism (CVE)

According to the FBI, a violent extremist is a person who advocates for, intends to engage in, engages in, or supports ideologically motivated terrorist activities in furtherance of political or social objectives.

In the effort to prevent violent extremism the Administration seeks to fulfill three main objectives:

- I. Enhance Federal involvement with and support to local communities that may be the target of violent extremists.
- II. Strengthen government and law enforcement capabilities for preventing violent extremism.
- III. Counter violent extremist propaganda while promoting our ideals and values.

Government and law enforcement efforts to counter violent extremism should be understood as dual-purpose. Officials should engage communities about security issues to raise awareness, establish partnerships, and empower local stakeholders, while encouraging community integration through platforms that deal with CVE and non-CVE related issues alike.

Applicable Programs for CVE

The following federal programs and are available to assist state and local governments, law enforcement, and community efforts on a variety of issues, including Countering Violent Extremism.

Office of Civil Rights and Civil Liberties (CRCL) - DHS

- Regular location-based meetings include representatives from federal, state, and local government agencies as well as individuals from the private sector and community leaders whose communities have civil rights concerns.

The Somali-American Initiative—DHS

- This initiative has involved Department of Homeland Security officials engaging Somali communities and organizations. Issues discussed in these meetings have included fighting in the Horn of Africa and other items relevant to the local Somali communities.

Youth Programs—DHS, DOJ

- A variety of youth programs may be used for purposes of locally-based initiatives to facilitate the integration of youth minority groups into the community.

Building Communities of Trust Initiative (BCOT)—DOJ

- This is a locally-based initiative which provides guidance for the development of trust among three sets of actors—fusion centers, law enforcement, and the communities in which they operate.

Further Reference Materials:

Department of Homeland Security—www.dhs.gov/cve

Civil Rights and Civil Liberties Training Guide—<http://www.dhs.gov/xlibrary/assets/cve-training-guidance.pdf>

Fusion Process Program/Fusion Liaison Officer—http://www.ncirc.gov/documents/Fusion_Process_Catalog_of_Services.pdf

Minneapolis-St. Paul, Minnesota "Blue Print for Action"

http://www.ci.minneapolis.mn.us/www/groups/public/@health/documents/webcontent/convert_278139.pdf

Applicable Grants for CVE

The following grants have been used by state and local government and law enforcement personnel to address Countering Violent Extremism in their communities. Of note, the FY 12 DHS grant guidance listed these grants as applicable for CVE purposes. The below information includes the title of the grant, the Catalog of Federal Domestic Assistance (CFDA) number and the federal agency/office that sponsors the grant, as of February 17, 2012:

- State Homeland Security Program (SHSP) —CFDA No. 97.073— Department of Homeland Security
- State and Local Anti-Terrorism Training (SLATT) —CFDA No. 16.614— Department of Justice
- Community –Based Violence Protection Program –CDA No. 16.123- Department of Justice
- Public Safety Partnership and Community Policing Grants —CFDA No. 16.710— Department of Justice
- Edward Byrne Memorial Justice Assistance Grant Program —CFDA No. 16.738— Department of Justice
- Civil Rights training and Advisory Services –CFDA No. 84.004- Department of Education

Local CVE Success Stories

.....*Minneapolis-St. Paul, Minnesota* Recognizing that youth violence is a public health epidemic that requires a holistic, multi-faceted response, Minneapolis has promoted an “enterprise-wide” approach to the challenge. Drawing on a mix of law enforcement and public health strategies, the city, in partnership with a host of community stakeholders, created the “Blueprint for Action Plan.”

The Blueprint’s goals are, to connect every youth with a trusted adult, to intervene at the first sign that youth are a risk for violence, to restore youth who have gone down the wrong path, and unlearn the culture of violence in the community. The Minneapolis Police Department is actively involved in community outreach initiatives and has fulltime liaisons to the different ethnic communities. In 2009, the city established the Neighborhood and Community Relations Department staffed with outreach specialists who speak several of the native languages.

.....*New York, New York* The New York City Police Department (NYPD) is involved in outreach efforts that impact the city’s diverse communities. NYPD’s Community Affairs Bureau, New Immigrant Outreach Unit, works with several of these ethnic groups, and institutes the following objectives:

Initiate programs that enhance the relationship between the immigrant communities and the police, initiate programs that address the needs and concerns of the immigrant communities, encourage participation in community programs, reduce fear by establishing open lines of communication and encourage dialogue, and educate the new immigrant communities on Rights and Responsibilities. The New Immigrant Outreach Unit also offers “terrorism awareness training” as one of its community participation programs. The NYPD has provided this training to 15,000 community members.

.....*Los Angeles, CA* – The Los Angeles County Sheriff’s Department (LASD) has developed an outreach program for the Muslim Community in Los Angeles County. It has grown to include a training program for the Muslim community on law enforcement issues such as hate crimes, domestic violence, gangs and identity theft. In addition to training and engaging with the community, the Muslim Community Affairs unit also trains Department members about Islam, Muslims, and related cultures, customs, and beliefs.

.....*Los Angeles, CA* The Los Angeles Police Department (LAPD) has established community forums hosted by the Department’s Chief to bring together community leaders and police from throughout the greater Los Angeles area to enable the LAPD to better understand how it can protect and serve their communities. LAPD maintains that community mobilization, an essential part of fighting crime, is particularly important when applied to populations that may feel targeted by society or the police.

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, CLASSIFIED and UNCLASSIFIED, threat-related information;
 - Building analytic capacity at the grass-roots level by supporting state and major urban area 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 may 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 better engage with their communities and on cultural demystification.
- 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 academies.

Countering Violent Extremism (CVE) Talking Points

- DHS's efforts to counter violent extremism (CVE) are based on the understanding that local authorities and community members are best able to identify those individuals or groups residing within their communities exhibiting dangerous and violent behaviors associated with extreme ideological beliefs.
- Today, the Department operates with the understanding that as it relates to domestic violent extremism we face the greatest terrorist risk from those extremists who have either been recruited by Al-Qa'ida or its affiliates or inspired by their ideology.
- However, we also know that violent extremism can be inspired by various religious, political, or other ideological beliefs.
- Recognizing this, DHS has designed a CVE approach that applies to all forms of violent extremism, regardless of ideology.
- Through a variety of analytic, research, outreach and training efforts, DHS works closely with state, local, tribal, and territorial law enforcement, other local government organizations, and community groups to incorporate efforts to counter violent extremism into pre-existing community-based violent crime prevention efforts.
- On December 8, 2011, the White House released the Strategic Implementation Plan (SIP) for the Administration's CVE Strategy, which 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 DHS CVE Approach, and in turn the SIP, were both informed based on the recommendations from the HSAC CVE Working Group that were issued in August, 2010.
- The Department is working with its Federal, State, Local, Tribal, and Territorial partners to fully integrate CVE awareness into the daily activities of law enforcement and local communities nationwide by building upon pre-existing partnerships and their existing practices, such as community policing, that have proven to be successful for decades.
- DHS was and continues to work closely with the White House, NCTC, DOJ, and the FBI to develop and implement the SIP. Efforts include the following:

Better Understanding Violent Extremism through Analysis and Research

- DHS has conducted extensive analysis and research to better understand the threat of violent extremism in order to support State and Local law enforcement, fusion centers, and community partners with the knowledge needed to identify behaviors and indicators of violent extremism, and prevent violent crime in their communities.
- This includes over 75 case studies and assessments produced by the DHS Office for Intelligence and Analysis (I&A) since 2009 on homegrown violent extremist activities and potential material support activities in the U.S. on behalf of violent extremist groups or causes, including an in-depth study that looks at the common behaviors associated with 62 cases of Al-Qa'ida-inspired violent extremists.
- DHS/I&A and Europol are finalizing a joint case study on the 2011 Norway terrorist attacks, including an extensive analysis of the Anders Breivik manifesto, in order to help law enforcement understand what the behaviors and indicators of violent extremism were leading up to the attacks.
- DHS's Science and Technology Directorate (S&T) has produced a series of reports that have informed CVE work on Hot Spots of Terrorism and Other Crimes, Characteristics of

American Communities Where Terrorists Lived, Planned, and Conducted Their Attacks, and Organizational Dynamics of Far-Right Hate Groups in the United States: Comparing Violent to Non-Violent Organizations.

- DHS/S&T and the National Consortium for the Study of Terrorism and Responses to Terrorism at the University of Maryland completed research on factors contributing to violent extremism and how to build community resilience to violent extremism among youth in the Somali community in Minnesota.
- DHS/S&T is conducting a series of focus groups with State and Local law enforcement officers at fusion centers and communities, to better identify their information and training needs; 20 locations have been selected and focus groups will begin on May 21, 2012.

Integrating CVE into Local Efforts to Prevent Violence through Training and Grant Prioritization

- **Overall Training:** DHS is in the final stages of implementing a CVE training for Federal, State, Local, and Correctional Facility law enforcement officers, as well as a training block for State Police Academies. The key goal of the training is to help law enforcement recognize the indicators of violent extremist activity and distinguish between those behaviors that are potentially related to crime and those that are constitutionally protected or part of a religious or cultural practice.
 - **State and Local Training:** DHS is working with the Los Angeles Police Department (LAPD), Major Cities Chiefs Association (MCCA), and the National Consortium for Advance Policing (NCAP) to finalize a continuing education CVE curriculum for state and local law enforcement—the first pilot was held on Jan. 26, 2012 in San Diego, CA and the next pilot will be in Minneapolis at the end of July. The curriculum will be available online before the end of 2012. The Major Cities Chiefs Association also passed a motion to adopt and implement the DHS CVE curriculum in their training academies.
 - **Police Academy Training Block:** DHS is working with the International Association of Chiefs of Police (IACP) to develop CVE curriculum for the recruit and field training officer (FTO) level which will be introduced into Police Academies and posted on an internet based platform before the end of 2012.
 - **Federal Training:** The Federal Law Enforcement Training Center (FLETC) has finalized a CVE curriculum for federal law enforcement that has been integrated into their existing training for new recruits. On February 16, 2012, DHS/FLETC hosted a full day symposium on this CVE curriculum and it is now incorporated in FLETC's training curriculum.
 - **Correctional Facility Training:** DHS is finalizing CVE awareness training for Correctional Facility, Probation, and Parole Officers in collaboration with the Interagency Threat Assessment Coordination Group (ITACG), Bureau of Prisons (BOP), and National Joint Terrorism Task Force (NJTTF)—the training was piloted on March 28, 2012 in the Maryland Public Safety and Corrections Training Center. The next pilot will take place on July 18, 2012 in Orange County, CA. FEMA is also developing a curriculum for rural correctional facility management.
 - **Training Standards:** Ensuring that State and Local law enforcement have access to operationally accurate and appropriate training is a top priority. DHS released the *CVE Training Guidance and Best Practices*, which was sent to all state and local partner grantors and grantees thereby tying to grant guidance policy on October 7, 2011. Both FEMA and FLETC are currently co-leading a DHS working group to determine how

CVE training offered by the Department and local partners is in line with DHS policy, that CVE trainers are accredited, and that state and local are held accountable for grant dollars that may be spent on CVE training.

- **Cultural Demystification Training:** DIIS is training local law enforcement on cultural demystification and how to best engage with communities via DHS CRCL's 46 separate training events. CRCL is integrating its training in to all CVE curriculum and training efforts.
- **Grants:** DIIS incorporated language into FY12 grant guidance that prioritizes CVE and allows funds to be used in support of State and Local CVE efforts.

Working with Local Communities and International Partners

- DHS works with non-governmental, state and local government, community, State and Local law enforcement, private sector and academic stakeholders, such as the DHS Homeland Security Advisory Council's (HSAC) CVE Working Group, which provided input that informed the DHS CVE approach.
- DHS hosted 50 State and Local law enforcement officials for a meeting at the White House on January 18, 2012 along with DOJ, FBI, and NCTC to hear feedback on how the federal government could better support their local CVE efforts.
- DIIS has also made significant advancements in operational CVE exchanges with international partners. For the past year, DHS, NCTC, DOJ, and the FBI, along with Europol and European Union partners, have held extensive discussions which have focused on exchanging: 1) case studies on specific instances of violent extremist activity and behaviors and indicators of violent extremism; 2) strategies used by local law enforcement to combat violent extremism; and 3) best practices in the area of CVE training.
 - These discussions also explored how the internet and social media is used to facilitate violent extremist activity in that it is used as a tool for those terrorist organizations seeking to recruit individuals for violent activities and/or as a communication conduit for those seeking to inspire individuals to commit acts of violence. This has included the sharing of over a dozen case studies and exchanging training and fusion center best practices.
 - DHS, Europol, and EU partners have developed a joint case study on the 2011 Norway attacks, including extensive analysis of the Anders Breivik manifesto. DIIS and Europol are also finalizing joint reports on training, and fusion center best practices, which will be distributed to law enforcement in the EU and the U.S.
 - **Success Story:** DHS/Europol attended a briefing at the Pennsylvania Criminal Intelligence Center (PaCIC) on January 20, 2012 on how software is being used to counter-child pornography. French law enforcement was given access to this software, which led to an arrest of one of the largest child pornography sharing targets in Paris.

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

Page 10 of 11
Withheld pursuant to exemption
Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 11 of 11
Withheld pursuant to exemption
Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

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

Page 1 of 6

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 6

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 6

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 4 of 6

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 5 of 6

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 6 of 6

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 9

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 9

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 9

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 4 of 9

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 5 of 9

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 6 of 9

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 7 of 9

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 8 of 9

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 9 of 9

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

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

Page 1 of 1

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

FACT SHEET: STRATEGIC IMPLEMENTATION PLAN FOR THE NATIONAL STRATEGY ON EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

“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 two years ago on our service members at Fort Hood.”

*– President Barack Obama
August 3, 2011*

In August 2011, President Obama approved the National Strategy for Empowering Local Partners to Prevent Violent Extremism in the United States (the “Domestic CVE Strategy”), which is the first U.S. Government strategy to address ideologically-inspired radicalization to violence in the homeland. Today we are releasing a Strategic Implementation Plan, which will serve as the blueprint for how we will implement the Domestic CVE Strategy. As such, the plan lists the specific current and future actions the U.S. Government will take in support of the Domestic CVE Strategy’s locally-focused, community-based approach to preventing violent extremism in the United States.

- Both the Domestic CVE Strategy and the Strategic Implementation Plan prioritize al-Qa’ida and its affiliates and adherents as the preeminent terrorist threat we face today. However, our approach applies to all forms of violent extremism. As the tragedy in Norway shows, free societies face a variety of terrorist threats. Our own experience with the Oklahoma City bombing underscores this point.
- Both the Domestic CVE Strategy and the Strategic Implementation Plan emphasize that communities are the solution not the problem; they are on the frontlines and best positioned to push back against violent extremists. Actions and statements that promote hatred or cast suspicion toward entire communities reinforce violent extremist propaganda and feed the sense of disenchantment that may spur violent extremist radicalization.

Our Ultimate Goal is to prevent violent extremists and their supporters from inspiring, radicalizing, financing, or recruiting individuals or groups in the United States to commit acts of violence.

Our Approach underscores the strength of communities. We are fortunate that our experience with community-based problem solving, local partnerships, and community-oriented policing provides a basis for addressing violent extremism as part of a broader mandate of community safety. We therefore are building our efforts from existing structures, while creating capacity to fill gaps as we implement programs. Rather than creating a new architecture of institutions and funding, we are utilizing successful models, increasing their scope and scale where appropriate. Specifically, the Strategic Implementation Plan provides detailed information on our three main lines of action: (1) Enhancing Federal engagement with and support to local communities; (2) Building expertise for countering violent extremism; and (3) Countering violent extremist propaganda while promoting our ideals.

- **Enhancing Engagement.** 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 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.** 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.

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.

The Role of Fusion Centers in Countering Violent Extremism (CVE)

Overview

The threat posed by violent extremism is neither constrained by international borders nor limited to any single ideology. 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. 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; helping frontline personnel understand terrorist and criminal threats they could encounter in the field. For fusion centers to engage ineffective information sharing, they also protect the privacy, civil rights, and civil liberties by empowering frontline personnel to differentiate between behaviors and indicators that may be associated with violent extremism and constitutionally protected behavior. Fusion centers play a crucial role in CVE by providing grassroots intelligence, analytic, and information sharing capabilities within the state and local environment to help identify and mitigate threats.

Role of Fusion Centers

Fusion centers play an important role in CVE efforts through their normal day-to-day operations, including gathering, analyzing, and sharing threat information. The Department is continuing to support fusion centers as they share information to support their law enforcement, public safety, and private sector partners' efforts to counter violent extremism, including:

- Building grassroots intelligence and analytic capabilities within the state and local environment so state and local 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 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 partners to help inform frontline personnel 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 state and local partners 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 community-policing efforts.

For More Information

For more information on fusion centers, please visit <http://www.dhs.gov/fusioncenters>, and for more information on DHS's approach to countering violent extremism, please visit <http://www.dhs.gov/cve>.

Background on CVE

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 communities as they play a vital role in countering violent extremism.
- **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 accordance with the *Empowering Local Partners to Prevent Violent Extremism in the United States*, 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 must be vigilant in identifying, predicting, and preempting new threats of violent extremism. This necessitates ongoing research and analysis, as well as exchanges with individuals, communities, and government officials who work on the front lines to counter the threats we face. We are also building robust programs to train frontline personnel on the identification of behaviors that are potentially indicative of terrorist or other criminal activity, raise public awareness of indicators of terrorism and violent crime, and emphasize the importance of reporting suspicious activity to the proper law enforcement authorities. Furthermore, we must ensure that communities, the government, and law enforcement receive accurate, intelligence-based information about the dynamics of violent extremism. Misinformation about threats, coupled with poor training, can harm our security by providing our stakeholders with inaccurate information 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.

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 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

The Role of Fusion Centers in Countering Violent Extremism (CVE)

Overview

The threat posed by violent extremism is neither constrained by international borders nor limited to any single ideology. 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. 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; helping frontline personnel understand terrorist and criminal threats they could encounter in the field. For fusion centers to engage ineffective information sharing, they also protect the privacy, civil rights, and civil liberties by empowering frontline personnel to differentiate between behaviors and indicators that may be associated with violent extremism and constitutionally protected behavior. Fusion centers play a crucial role in CVE by providing grassroots intelligence, analytic, and information sharing capabilities within the state and local environment to help identify and mitigate threats.

Role of Fusion Centers

Fusion centers play an important role in CVE efforts through their normal day-to-day operations, including gathering, analyzing, and sharing threat information. The Department is continuing to support fusion centers as they share information to support their law enforcement, public safety, and private sector partners' efforts to counter violent extremism, including:

- Building grassroots intelligence and analytic capabilities within the state and local environment so state and local 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 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 partners to help inform frontline personnel 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 state and local partners 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 community-policing efforts.

For More Information

For more information on fusion centers, please visit <http://www.dhs.gov/fusioncenters>, and for more information on DHS's approach to countering violent extremism, please visit <http://www.dhs.gov/cve>.

Background on CVE

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 communities as they play a vital role in countering violent extremism.
- **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 accordance with the *Empowering Local Partners to Prevent Violent Extremism in the United States*, 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 must be vigilant in identifying, predicting, and preempting new threats of violent extremism. This necessitates ongoing research and analysis, as well as exchanges with individuals, communities, and government officials who work on the front lines to counter the threats we face. We are also building robust programs to train frontline personnel on the identification of behaviors that are potentially indicative of terrorist or other criminal activity, raise public awareness of indicators of terrorism and violent crime, and emphasize the importance of reporting suspicious activity to the proper law enforcement authorities. Furthermore, we must ensure that communities, the government, and law enforcement receive accurate, intelligence-based information about the dynamics of violent extremism. Misinformation about threats, coupled with poor training, can harm our security by providing our stakeholders with inaccurate information 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.

- 1) Thank you and recognitions
- 2) Let me start by explaining what Global Engagement is to provide context for our approach to CVE. I'll then discuss how we think about the issue as one among a number of community safety challenges. Finally, I will outline our three main areas of CVE activity.
- 3) Global Engagement
 - a) Global Engagement Directorate established by the President and charged with "comprehensive engagement policies that leverage diplomacy, communications, international development and assistance, and domestic engagement and outreach in pursuit of a host of national security objectives, including those related to the homeland."
 - b) Global not just in terms of geography, but in the kinds of partnerships and comprehensive relationships we build, recognizing that the major challenges we face are too complex for any one actor
 - c) Objective—to build diverse coalitions to address challenges. A move away from unilateralism and expansion beyond state-to-state. New partners and new ways of doing things. Different disciplines, different skill sets, better solutions.
 - d) Importantly, it takes advantage of the unique value added of government as a facilitator, convener, and network broker.
 - i) We have vast networks, and can bring people from many different perspectives and backgrounds together
 - ii) Bollywood story
- 2) Two Examples—one global, and a second local
 - a) The Global Alliance of Clean Cookstoves
 - i) Exposure to smoke from traditional cookstoves and open fires (the primary means of cooking & heating for nearly 3 billion people in the developing world) causes 1.9 million premature deaths annually, impacting women and children in particular. Cookstoves also increase pressure on local natural resources.
 - ii) The U.S. Department of State led the formation of a public-private partnership—involving Shell Oil, Morgan Stanley, and numerous local NGOs—to generate a global campaign to raise awareness of the danger and facilitate transition to clean cookstove technology in countries like El Salvador, Peru, and most recently Tanzania

- b) Very local level example—Working with Somali youth in London to impact media portrayals, built a mentorship/training program on grassroots organizing with at least ten different partners (UK Government included)
- 3) This approach to problem solving is something we have been doing domestically for decades—community-based problem solving, comprehensive relationships, local level
- a) Community-policing—focuses on the use of wide ranging partnerships and problem solving to proactively address conditions that give rise to crime, social disorder, and fear of crime.
 - i) Collaborative partnerships include other government agencies, community members and organizations, NGOs, business, media, and others
 - b) Weed and Seed—DOJ delinquency prevention strategy, which develops partnerships among law enforcement, social service providers, educators, and others to create comprehensive, multi service programs that address vulnerabilities to delinquency and gang participation
 - c) School shootings
 - i) Shooting at Columbine H.S. as a turning point—April 20, 1999. Thirteen people killed before the two perpetrators committed suicide
 - ii) Prior to this, we were less sensitive to the threat—often seen as “blowing off steam,” and concerns about getting people in trouble by reporting
 - iii) Now, very different reactions—built a new awareness, local networks of trust.
 - (1) Recognition that need integrated approach and cooperation and partnerships between schools and organizations outside schools, including law enforcement, social services and mental health providers, courts, community organizations, families, religious organizations and many others
- 4) Now we are working to apply the approach of global engagement, and our experience in building diverse local networks for problem solving, to address the challenge of ideologically inspired violence and radicalization
- a) We thus are building from established practices. Rather than inventing new CVE architecture, we are working through preexisting networks and trusted relationships, while establishing and building new ones where necessary. We are trying to mainstream this work as part of our efforts to promote community safety, rather as a standalone enterprise.

- b) Many of our potential partners are not involved in national security issues and wouldn't see themselves as playing a role. They don't speak the same language or use CT frames of reference. More effective to view CVE as part of community safety in general.
 - i) As a parent, my reaction if someone asked me to support CVE.
 - ii) Teachers
 - iii) Other government departments
- 5) In addressing violent extremism in the U.S., it is important to understand that we face a variety of threats, not just al-Qaeda, and as a result our CVE activities must be flexible enough to address multiple forms of violent extremism as well as new threats as they emerge.
 - a) From 2001-2010, there were numerous disruptions for non-al Qaeda terrorism, including plots and material support.
 - b) Diverse array of groups.
 - (1) Violent militia extremism and sovereign citizen groups
 - (a) In March 2010, nine militia arrests in Michigan.
 - (b) March 2011, five militia and sovereign citizens arrested for weapons violations and threats against a judge and law enforcement
 - (2) Violent white supremacists—April 2011, four indicted and charged with different violations for firebombing the home of a mixed race couple in Arkansas
 - (3) Violent anti-abortion groups. November 2010, Army of God member pled guilty to one count of distributing information related to explosives, destructive devices and weapons of mass destruction.
 - c) Having said this, we must prioritize our efforts and resources, and al Qaeda and its adherents remain the most significant threat to the security of our country.
 - i) When we assess this prioritization, we look at three factors:
 - (1) Intent—stated or implied purpose of a group to engage in an act of terrorism
 - (2) Capability—ability to conduct an attack based on resources, skills, historical actions, or presence

- (3) Posture—preparation of a group to conduct an attack
- ii) Without belaboring the point, AQ clearly rates high on all of these measures
 - (1) They don't hide their intentions—videos, Inspire Magazine, etc.—Awlaki, Adam Ghadan, and others have called on American citizens and residents to attack. UBL was still plotting, mass transit attack on the 10th anniversary of 9/11
 - (2) And they have proven their capability and posture, including several aviation plots by AQAP that fortunately failed.
- iii) The past several years have seen increased numbers of American citizens and residents inspired by AQ's ideology and involved in terrorism. Some have traveled overseas to train or fight, while others have been involved in supporting, financing, or plotting attacks in the homeland
- d) But patterns are difficult to come by, and in some ways differ from the experiences in Europe
 - i) Geographically dispersed throughout the country—Texas; Portland, Oregon; the Washington, DC area; NYC; and others
 - ii) Dozens involved over the past decade, but we don't find large networks—very small groups, generally a few individuals
 - iii) And wide range of individuals, making it difficult to profile—
 - (1) from Jihad Jane, who pled guilty of conspiring to kill a Swedish cartoonist,
 - (2) to Omar Hammami, a convert to Islam from Alabama who went on to become a military commander in al-Shabab,
 - (3) to Zazi, a legal permanent resident of the U.S. from Afghanistan who pled guilty to an al-Qaeda linked plot to bomb the NYC subway system.
- e) The number of such individuals is thus far limited, but we remain concerned, much in the way we are concerned about other community safety issues where there are relatively few perpetrators but enormous consequences. Take school shootings as an example.
 - i) Since September 2001, we have had around 60 school shootings. In the vast majority of incidents, between 0 and 2 were killed; in only 7 incidents were three or more people killed. And exceptions, like Virginia Tech, where 32 were killed. For

- comparison, during that same period, there were 41 terrorism disruptions linked to AQ and its adherents.
- ii) There is no geographic concentration; incidents are spread throughout the country
 - iii) It is difficult to profile. Many shooters told Secret Service investigators that they were driven by alienation or persecution, but many students experience these things, making it less useful.
 - iv) Many more individuals are killed in car accidents and gang violence, but we still take school shootings as a threat to community safety seriously
- f) We have responded to school shootings and other threats to community safety by engaging communities and building local networks of trust for collaborative problem solving. And we are taking a similar approach in addressing domestic violent extremism, focused on raising the awareness of everyone.
- 6) There are three pillars of our activity—all part of building diverse networks
- a) Engagement with several different groups and communities
 - i) Communities targeted by violent extremists for radicalization
 - (1) Ensure that where there are already relationships with the federal government, we work through those, dealing with CVE as one among a variety of community safety issues.
 - (2) Where there are no or weak relationships, then we need to build these, not only because of CVE but because this is good governance. Trust is essential for solving an array of challenges, from gang violence, to drug addiction, to school safety, to civil rights. Good governance builds up trust that applies across issue areas. This means an expanded role in engagement across our entire government, involving Health and Human Services and others.
 - (3) In our effort to counter violent extremism we must remain engaged in the full range of community concerns and interests and do not narrowly build our relationships on national security issues alone.
 - (a) So, for example, although we have begun working with the Somali community in Minneapolis on countering violent extremism, we also engage on a host of other issues.
 - (b) Somali parents, like parents everywhere, are concerned about school bullying.

- (i) An investigation in a Minneapolis school district found that, after a fight between eleven white and Somali students at a school, the district meted out disproportionate punishment to the students and that the school did not have appropriate policies, procedures and training to address harassment against Somali students.
 - (ii) DOJ and Department of Education reached a settlement agreement in which the district agreed to improve its policies and procedures on harassment and discipline.
- (4) In addressing CVE specifically, we engage communities for a number of reasons
 - (a) Raise awareness—NCTC community awareness briefing—the threat and challenge and what they can do to protect their families and loved ones. Communities have leveraged it in their own grassroots efforts.
 - (b) Understand concerns from communities about CVE related activities, and work to address them together
 - (c) Get advice and ideas about how to address the challenge, and the ways in which we can work together
- ii) Local government and law enforcement
 - (1) Often have stronger relationships and better understanding of local communities
 - (a) More likely to have trust
 - (b) More likely to be approached if an issue emerges; and
 - (c) Present as part of the communities, there day in and day out
- iii) NGOs, universities, others in civil society, such as interfaith groups, and private sector who may be able to support the communities that are being targeted
 - (1) Example from Diaspora Forum—individual noted that she wanted to communicate to broader audiences, but has no background or expertise in getting ideas out.
 - (2) Private sector has shown increased interest in becoming involved—Google formers conference at the end of June in Ireland
 - (3) Interfaith community—creating understanding, mitigating extremist arguments
- iv) And our close partners here today and their communities and networks

- (1) Example, the development of the Global Somali Diaspora network against violent extremism—offer up as a potential model for cooperation

b) Training

- i) Critical that our officials and local government and law enforcement understand the issue so that they know what it is, and what it isn't
- ii) We know that there are many trainers out there claiming to be experts, when they are far from it, and they promote a message that misguides people and weakens our national security by distracting people (Washington Monthly story)
- iii) We have formed an interagency working group on training. Among other areas of activity:
 - (1) Identify all CVE training and ensure it meets certain standards
 - (2) Identify community safety related training, where a CVE module could be included
 - (3) Develop a fully certified CVE training program that includes cultural competency, radicalization that leads to violence, and how to partner with communities and others
- iv) We have been expanding this training and will continue to do so, particularly with local officials and stakeholders. From October 2010-early March this year, for example, DHS offered this sort of training to more than 1,000 law enforcement and other government personnel across the country.

c) Challenging the narrative

- i) The narrative of terrorists—West is at war with Islam and anti-Muslim, and we need to challenge this by words and deeds.
 - (1) This means promoting an alternative narrative of what it means to be an American, and the ideals that unify us as a country, irrespective of race, religion, or creed. One of the strengths of our country is its diversity.
 - (2) It means continuing to vigorously protect civil rights and prosecute anti-Muslim hate crimes and ensuring that any community targeted by violent extremists for radicalization feel they are an essential part of the national fabric. And our Department of Justice has gone to court to protect the rights of Muslims.

- (3) And it means communicating to the general American public about what the threat is, and is not. It is not Islam and it is not Muslims. As the President stated, Bin Ladin was not a Muslim leader, he was a murderer.
 - (a) Actions and statements that cast suspicion towards entire communities because of the actions of a few or send messages to certain Americans that they are somehow less American because of their faith or how they look, reinforce violent extremist propaganda and feed the sense of disenchantment and disenfranchisement that may spur violent extremist radicalization.
- (4) This also has international implications. We live in a communications environment where you cannot separate the domestic from the international, where news about anti-Muslim antics in the U.S. spread to other countries, sometimes with deadly consequences.
 - (a) Pastor Jones burned the Koran in Florida and violent protests erupted in Afghanistan. He later announced he was headed to Dearborn, MI to protest in front of the largest mosque in North America. Rumors about possible Koran burning or burning an effigy of the Prophet.
 - (b) The reaction of the entire Dearborn community serves as a model for building cross-cutting networks in addressing a challenge. Explain the reaction.

7) Conclusion

- a) The President has been concerned about this challenge since day one. In fact, my first briefing to him on this topic was one month after he took office when the administration was just settling in.
- b) The President is someone who recognizes the value of collaborative partnerships; that is the purpose of global engagement. It is about building coalitions to address challenging problems. We recognize that this is not something government can do alone; it takes a diverse network of individuals and organizations, each of which brings unique skills and value added.
- c) At home, we are building these networks and these relationships, though there remains much work to be done.
- d) Importantly, our understanding of how we approach the challenge has benefited enormously from our partnerships and exchanges with our British, Dutch and German colleagues, and many others. In fact, prior to my current role at the White House, I spent 18 months in the UK, where our British colleagues generously allowed us

opportunities to witness their counter-radicalization efforts first hand to assess whether lessons can applied to our Homeland. This was invaluable and has allowed us to build on the experiences of our close friends.

- e) We will continue to do so at conferences like this, and we hope many more.
- f) Thank you

Page 01 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 25 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 26 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 27 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 28 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 29 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 30 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 31 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 32 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 33 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 34 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 35 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 36 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 37 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 38 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 39 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 40 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 41 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 42 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 43 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 44 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 45 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 46 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 47 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 48 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 49 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 50 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 51 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 52 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 53 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 54 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 55 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 56 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 57 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 58 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 59 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 60 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 61 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 62 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 63 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 64 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 65 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 66 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 67 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 68 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 69 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 70 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 71 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 72 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 73 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 74 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 75 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 76 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 77 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 78 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 79 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 01 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 25 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 26 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 27 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 28 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 29 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 30 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 31 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 32 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 33 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 34 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 35 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 36 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 37 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 38 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 39 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 40 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 41 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 42 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 43 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 44 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 45 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 46 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 47 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 48 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 49 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 50 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 51 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 52 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 53 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 54 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 55 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 56 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 57 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 58 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 59 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 60 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 61 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 62 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 63 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 64 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 65 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 66 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 67 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 68 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 69 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 70 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 71 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 72 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 73 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 74 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 75 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 76 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 77 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 78 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 79 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 01 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 25 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 26 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 27 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 28 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 29 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 30 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 31 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 32 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 33 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 34 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 35 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 36 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 37 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 38 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 39 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 40 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 41 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 42 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 43 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 44 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 45 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 46 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 47 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 48 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 49 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 50 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 51 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 52 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 53 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 54 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 55 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 56 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 57 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 58 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 59 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 60 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 61 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 62 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 63 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 64 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 65 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 66 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 67 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 68 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 69 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 70 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 71 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 72 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 73 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 74 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 75 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 76 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 77 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 78 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 79 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 01 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 25 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 26 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 27 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 28 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 29 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 30 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 31 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 32 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 33 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 34 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 35 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 36 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 37 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 38 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 39 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 40 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 41 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 42 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 43 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 44 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 45 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 46 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 47 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 48 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 49 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 50 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 51 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 52 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 53 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 54 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 55 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 56 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 57 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 58 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 59 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 60 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 61 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 62 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 63 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 64 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 65 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 66 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 67 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 68 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 69 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 70 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 71 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 72 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 73 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 74 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 75 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 76 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 77 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 78 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 79 of 79

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

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 6 of 8

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

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 6 of 8

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: Snyder, Nathaniel (b)(6)
(b)(6)
To: "Snyder, Nathaniel"
(b)(6)
BCC: "Gersten, David" (b)(6)
(b)(6)
"Shora, Kareem"
(b)(6)
"Shora, Nawar <
(b)(6)>
"Presswalla, Jend
(b)(6)
"Selim, George <
(b)(6)>

Subject: National Strategic Implementation Plan to Empowering Local Partners to Prevent Violent Extremism in the US

Date: 2011/12/08 16:00:00

Importance: High

Priority: Urgent

Type: Note



Dear Department of Homeland Security Partners,

Today, President Obama released the Strategic Implementation Plan (SIP) to the National Strategy on Empowering Local Partners to Prevent Violent Extremism in the United States (attached). The SIP is the blueprint for how we will implement the Domestic Strategy on Countering Violent Extremism (CVE), the first U.S. Government strategy to address violent extremism in the Homeland. The SIP lists the current and future actions the U.S. Government will take in support of a locally-focused, community-based approach, in three broad areas: (1) enhancing engagement with and support to local communities; (2) building government and law enforcement expertise; and (3) countering violent extremist propaganda while promoting our ideals. This is the first U.S. Government strategy and implementation plan to address ideologically-inspired violent extremism in the homeland.

This SIP is a follow up to the National Strategy on Empowering Local Partners to Prevent Violent Extremism in the United States, which was released by the White House in

August 2011. DHS, along with interagency partners, worked with the Administration to develop this SIP.

For additional information on the DHS approach to CVE, see our [DHS CVE Fact Sheet](#).

Thank you for all you do to help keep our nation safe and secure.

Sender: Snyder, Nathaniel (b)(6)
(b)(6)

Recipient: "Snyder, Nathaniel" (b)(6)
(b)(6)
"Gersten, David" <(b)(6)>
(b)(6)
"Shora, Kareem" <(b)(6)>
(b)(6)
"Shora, Nawar" <(b)(6)>
(b)(6)
"Presswalla, Jenn" <(b)(6)>
(b)(6)
"Selim, George" <(b)(6)>
(b)(6)
"Crawley, Ayn" <(b)(6)>

Sent Date: 2011/12/08 16:00:24

Delivered Date: 2011/12/08 16:00:00

From: Snyder, Nathaniel (b)(6)
(b)(6)

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

BCC: (b)(6)

[Redacted content]

(b)(6)

Subject: National Strategic Implementation Plan to Empowering Local Partners to Prevent Violent Extremism in the US

Date: 2011/12/08 14:53:00

Importance: High

Priority: Urgent

Type: Note



Dear Department of Homeland Security Partners,

Today, President Obama released the Strategic Implementation Plan (SIP) to the National Strategy on Empowering Local Partners to Prevent Violent Extremism in the United States (attached). The SIP is the blueprint for how we will implement the Domestic Strategy on Countering Violent Extremism (CVE), the first U.S. Government strategy to address violent extremism in the Homeland. The SIP lists the current and future actions the U.S. Government will take in support of a locally-focused, community-based approach, in three broad areas: (1) enhancing engagement with and support to local communities; (2) building government and law enforcement expertise; and (3) countering violent extremist propaganda while promoting our ideals. This is the first U.S. Government strategy and implementation plan to address ideologically-inspired violent extremism in the homeland.

This SIP is a follow up to the National Strategy on Empowering Local Partners to Prevent Violent Extremism in the United States, which was released by the White House in August 2011. DHS, along with interagency partners, worked with the Administration to develop this SIP.

For additional information on the DHS approach to CVE, see our DHS CVE Fact Sheet.

Thank you for all you do to help keep our nation safe and secure.

Sender: Snyder, Nathaniel (b)(6)
(b)(6)

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

(b)(6)

Sent Date: 2011/12/08 14:53:47

Delivered Date: 2011/12/08 14:53:00

Page 1 of 6
Withheld pursuant to exemption
Duplicate
of the Freedom of Information and Privacy Act

Page 2 of 6
Withheld pursuant to exemption
Duplicate
of the Freedom of Information and Privacy Act

Page 3 of 6
Withheld pursuant to exemption
Duplicate
of the Freedom of Information and Privacy Act

Page 4 of 6
Withheld pursuant to exemption
Duplicate
of the Freedom of Information and Privacy Act

Page 5 of 6
Withheld pursuant to exemption
Duplicate
of the Freedom of Information and Privacy Act

Page 6 of 6
Withheld pursuant to exemption
Duplicate
of the Freedom of Information and Privacy Act

Call with NYPD (b)(6) Deputy Commissioner of Training

March 1, 2012, 11:00 AM – 12:00 PM

Dial: 1-800-320-4330 // Conf Pin: 295830

PURPOSE:

- This call is to touch base and discuss ways to DHS can assist and support the NYPD in their training efforts.

BACKGROUND INFORMATION:

- NYPD Inspector Amin Kosseim was a member of the HSAC CVE Working Group and has been actively working with DHS on its CVE efforts.
- Inspector (b)(6) proactively reached out to Deputy Commissioner (b)(6) and informed him about the Department's efforts RE: CVE training and the approach it has been taking.
- The Deputy Commissioner is interested in learning more on what DHS is doing on CVE and resources available that would help NYPD.
- This is an introductory call, and will hopefully lead to closer collaboration on CVE efforts and training.

TALKING POINTS

- **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.

- 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.

ATTACHMENTS:

None.

PARTICIPANTS:

YOU

NYPD (b)(6) Deputy Commissioner of Training

NYPD Inspector (b)(6)

(b)(6) CTWG

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

From: (b)(6)
To: "Saupp, Kevin (b)(6)
"Diane Ragans (b)(6)
CC: "Snyder, Nathaniel (b)(6)
(b)(6)
Subject: Re: CVE panel
Date: 2012/03/23 17:41:15
Type: Note

This is the latest I have:

State and Local Support to Address Homegrown Violent Extremism

Session Description: Homegrown violent extremism (HVE) 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: 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.
- Hear about locally-led fusion center efforts to identify and address Homegrown 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 (b)(6)
Branch Chief, Federal Interagency Coordination
Department of Homeland Security

Office of Intelligence and Analysis
State and Local Program Office

Sender: Trelles D'Alemberte (b)(6)

Recipient: "Saupp, Kevin" (b)(6)
"Diane Raqans"
(b)(6)

Sent Date: 2012/03/23 17:41:07

Delivered Date: 2012/03/23 17:41:15

From: Bart R. Johnson (b)(6)
To: "Snyder, Nathaniel" (b)(6)
CC: "Simmons, Caroline" (b)(6)
Subject: RE: National Strategic Implementation Plan to Empowering Local Partners to Prevent Violent Extremism in the US
Date: 2012/01/09 09:51:08
Type: Note

I will have some other ideas for names.

From: Snyder, Nathaniel (b)(6)
Sent: Monday, January 09, 2012 9:44 AM
To: Bart R. Johnson
Cc: Simmons, Caroline
Subject: RE: National Strategic Implementation Plan to Empowering Local Partners to Prevent Violent Extremism in the US

Sure thing.

I am making some final edits on the agenda and will send that out as well.

It will still be a draft agenda, but will have more than enough detail for people to get a firm grasp of the day.

I will send you that along with the strategy and implementation plan first.

We'll have another email go out with more read-aheads but this should get people situated.

Good news about (b)(6) attending.

We are still working on bolstering out numbers so if you have any further ideas on additional participants that are within driving distance of NCR that would be great.

Thanks again,

-Nate

From: Bart R. Johnson (b)(6)
Sent: Monday, January 09, 2012 9:38 AM
To: Snyder, Nathaniel
Subject: RE: National Strategic Implementation Plan to Empowering Local Partners to Prevent Violent Extremism in the US

Nate:

Can you also send to me the other relevant information – IE the actual strategy – and also any other materials you believe would be useful to the members attending this meeting.

Thanks,

From: Snyder, Nathaniel (b)(6)
Sent: Thursday, December 08, 2011 2:54 PM
To: Snyder, Nathaniel
Subject: National Strategic Implementation Plan to Empowering Local Partners to Prevent Violent Extremism in the US
Importance: High



Dear Department of Homeland Security Partners,

Today, President Obama released the Strategic Implementation Plan (SIP) to the National Strategy on Empowering Local Partners to Prevent Violent Extremism in the United States (attached). The SIP is the blueprint for how we will implement the Domestic Strategy on Countering Violent Extremism (CVE), the first U.S. Government strategy to address violent extremism in the Homeland. The SIP lists the current and future actions the U.S. Government will take in support of a locally-focused, community-based approach, in three broad areas: (1) enhancing engagement with and support to local communities; (2) building government and law enforcement expertise; and (3) countering violent extremist propaganda while promoting our ideals. This is the first U.S. Government strategy and implementation plan to address ideologically-inspired violent extremism in the homeland.

This SIP is a follow up to the National Strategy on Empowering Local Partners to Prevent Violent Extremism in the United States, which was released by the White House in August 2011. DHS, along with interagency partners, worked with the Administration to develop this SIP.

For additional information on the DHS approach to CVE, see our DHS CVE Fact Sheet.

Thank you for all you do to help keep our nation safe and secure.

Sender: Bart R. Johnson (b)(6)
Recipient: "Snyder, Nathaniel (b)(6)
(b)(6)

"Simmons, Caroline (b)(6)

Sent Date: 2012/01/09 09:52:35

Delivered Date: 2012/01/09 09:51:08

Message Flags: Unread

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

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

Page 1 of 1

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Background

The White House strategy on countering violent extremism entitled, *Empowering Local Partners to Prevent Violent Extremism in the United States*, outlines the commitment of the Federal Government to support and help empower American communities and their local partners in their grassroots efforts to prevent violent extremism by:

- Improving support to communities, including sharing more information about the threat of radicalization;
- Strengthening cooperation with local law enforcement, who work with these communities every day; and
- Helping communities to better understand and protect themselves against violent extremist propaganda, especially online

DHS also released its approach to Countering Violent Extremism (CVE) which includes working with a broad range of partners 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. The DHS approach to CVE outlines three main objectives:

- Support and coordinate effort to better understand the phenomenon of violent extremism, including assessing the threat it poses to the Nation as a whole and within specific communities;
- Bolster efforts to catalyze and support non-governmental, community-based programs, and strengthen relationships with communities that may be targeted for recruitment by violent extremists; and
- Disrupt and deter recruited or individual or individual mobilization through support for local law enforcement programs, including information-driven, community-oriented policing efforts that for decades have proven effective in preventing violent crime.

In support of this strategy, DHS in partnership with the Department of Justice, the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence, and the National Counterterrorism Center (NCTC), hosted a *National CVE Workshop* designed to provide fusion center personnel and major city police department intelligence unit commanders with a better understanding of violent extremism and ongoing efforts to address the issue.

In addition, DHS partnered with the Los Angeles Police Department (LAPD) and the National Consortium for Advanced Policing (NCAP) to pilot a 24 hour CVE curriculum for law enforcement executives and frontline officers. The pilot took place in San Diego, CA from January 25-27 and included students from LAPD, Los Angeles Sheriff's Department, San Diego Police Department, San Diego Harbor Police, and surrounding jurisdictions. Community engagement practices, case studies on CVE, suspicious activity reporting (SAR), online violent extremist threats (including cyber), and enhancing community policing strategies were covered in the lesson plan.

Lastly, it is becoming more apparent that violent extremists are occupying and using online spaces and the virtual environment to execute criminal activity. DHS is looking to increase public awareness on these threats, as well as the associated tactics, techniques, and procedures associated with violent extremist threats. Further awareness training for state, local, territorial,

and tribal (SLTT) law enforcement and community stakeholders is needed to address these issues.

Scope

The following approach represents an integrated strategic awareness training program on violent extremists. Throughout this program, DHS will enhance SLTT law enforcement's ability to leverage actionable information such as, but not limited to: training on behaviors and indicators of terrorist threats, SAR processes and the NSI, HVE briefings/case studies (to include cyber), community policing, and public engagement tactics to increase stakeholder awareness of efforts to identify and counter violent extremism and terrorist/cyber threats.

Objectives/Deliverables

This effort includes the provision of awareness training and briefings on efforts to CVE, SAR, community policing, public engagement, cyber security/online violent extremist threats, cultural demystification, and HVE case studies.

The main objectives of these efforts include but are not limited to:

- Increase the awareness and understanding of cyber/online and violent extremist threats
- Ensure that stakeholders have the appropriate understanding and knowledge of behaviors and indicators of terrorist threats , as well as associated processes to report suspicious activities
- Increase the usage of public engagement and community policing methods and efforts
- Ensure that actionable information and training is consistent with DHS and White House policy, accurate, and accountable; and that it will inform future efforts
- Support the sharing of information between fusion centers and SLTT law enforcement
- Ensure that privacy, civil rights, and civil liberties are protected throughout these efforts
- Educate stakeholders that they have a role in building secure and resilient communities

Specifics

Delivery method(s) of the objectives may take the form through a combination of informational and interactive workshops and/or briefings. Regardless of method of application, information concerning the objectives will have to be tailored and applied on a regional basis. At a minimum, funding will be leveraged to support three (3) 24 hour CVE awareness training pilots in locations to be determined, and conducted in FY12. Each pilot should include approximately 45-50 local enforcement participants in locations selected by DHS. Additional regional efforts would be similar to the *National CVE Workshop* and potentially have training/briefing components—they would also need to be tailored to fit local needs and demands. Three (3) regional workshops would have to be completed in FY12.

Sub-IPC on CVE Training for Law Enforcement

March 1, 2012, 3:00 AM – 5:00 PM

BLDG 4; Conf Room 124 // Dial-In: 1 877-711-5292 // PIN: 870782

PURPOSE:

- Re-kick off the sub-IPC discussion on CVE Law Enforcement training.

BACKGROUND INFORMATION:

- This is the first sub-IPC on CVE Law Enforcement Training this year; Dan Sutherland (NCTC) will be re-kicking off the meeting with you. Both DHS-CTWG and NCTC are now chairing this sub-IPC.
- The major deliverable that came out of this group last year was the CVE Training Guidance that CRCL then issued with FEMA via an informational bulletin.
- CRCL has previously chaired this sub-IPC, and should be recognized for the work that they had previously done.
- There is a major emphasis on law enforcement training given recent issues; this group will be leveraged to coordinate interagency training efforts and bring best practices to the surface.
- It is clear that many departments and agencies (DOS, DOD, DHS, NCTC, DOJ(COPS), DOE, and others) have trainings and are developing trainings that will have an impact on law enforcement CVE efforts.
- Given the re-kick off of this sub-IPC, it will focus on immediate and long term deliverable goals, and this group will expand with participation.
- Jenny Presswalla and Nate Snyder will drive the agenda after you kick things off.

TALKING POINTS

- **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 be 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 led 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 Advanced 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 Glynnco, GA.
 - 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.

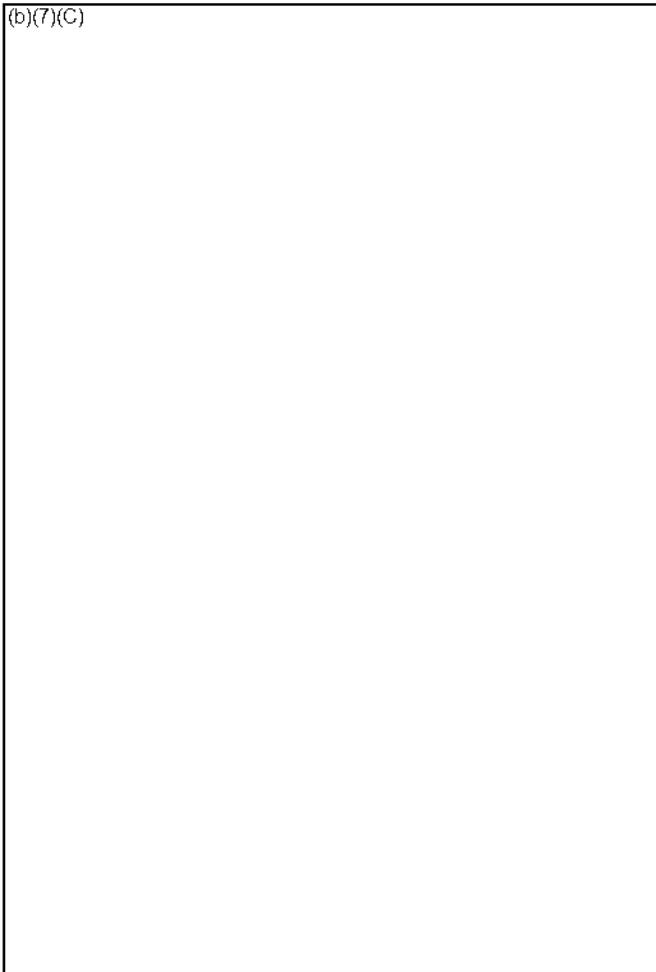
- The SIP Approach underscores the strength of community-based problem solving, local partnerships, and community-oriented policing. We are building our efforts from existing structures, while creating capacity to fill gaps as we implement programs.

ATTACHMENTS:

A. Agenda

PARTICIPANTS:

YOU



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

Page 1 of 1

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 01 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 25 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 26 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 27 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 28 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 29 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 30 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 31 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 32 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 33 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 34 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 35 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 36 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 37 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 38 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 39 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 40 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 41 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 42 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 43 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 44 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 45 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 46 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 47 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 48 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 49 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 50 of 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act