

#### GOAL 4.4: STRENGTHEN THE CYBER ECOSYSTEM

Our entire society, from government and law enforcement to the private sector and members of the public, must work collaboratively to improve our network defense. Ensuring a healthy cyber ecosystem will require collaborative communities, innovative and agile security solutions, standardized and consistent processes to share information and best practices, sound policies and plans, meaningful protection of privacy, civil rights, and civil liberties, and development of a skilled workforce to ensure those policies and plans are implemented as intended.

**We will pursue the following strategies to strengthen the cyber ecosystem:**

*Drive innovative and cost effective security products, services, and solutions throughout the cyber ecosystem* by working with domestic and international partners across the public and private spheres, and across the science and policy communities to identify promising technology, policy and standards that enable robust, trust-based, automated sharing of cybersecurity information and collective action to limit the spread of incidents and minimize consequences.

*Conduct and transition research and development, enabling trustworthy cyber infrastructure* by supporting initiatives to develop promising new security technologies and techniques including: 1) security automation techniques to facilitate real-time incident response; 2) interoperability to support security cooperation across sectors; and 3) privacy enhancing authentication to enable better system protection.

*Develop skilled cybersecurity professionals* by promoting cybersecurity knowledge and innovation, developing Department-wide human capital strategies, policies, and programs intended to enhance the DHS cyber workforce, and working with public and private sector partners to increase the pipeline of highly qualified homeland security professionals through academic and federal training programs.

*Enhance public awareness and promote cybersecurity best practices* by promoting *National Cybersecurity Awareness Month* and the *Stop. Think. Connect.™ Campaign*, which raise awareness through collaborative outreach efforts and distributing materials, resources, and tips to promote cybersecurity.

*Advance international engagement to promote capacity building, international standards, and cooperation* by working to establish and deepen relationships with foreign computer incident response teams both bilaterally and through participation in operationally-focused multilateral fora, such as the Forum for Incident Response and Security Teams.

# DEPARTMENT MISSIONS AND GOALS

## HIGHLIGHTED PERFORMANCE MEASURES

The table below presents a subset of the DHS performance measures associated with gauging results for Mission 4. For more information on these measures, along with a more extensive list of measures associated with this mission, please see the FY 2013–2015 Annual Performance Report at [http://www.dhs.gov/xabout/budget/editorial\\_0430.shtm](http://www.dhs.gov/xabout/budget/editorial_0430.shtm).

Mission 4: Safeguard and Secure Cyberspace				
Highlighted Performance Measures	Goal Alignment	Planned Targets		
		FY 2014	FY 2015	FY 2018
Percent of intelligence reports rated “satisfactory” or higher in customer feedback that enable customers to manage risks to cyberspace (AO)	4.1	94%	95%	95%
Percent of organizations that have implemented at least one cybersecurity enhancement after receiving a cybersecurity vulnerability assessment or survey (NPPD)	4.1	55%	60%	75%
Percent of traffic monitored for cyber intrusions at civilian Federal Executive Branch agencies (NPPD)	4.2	85.0%	87.0%	93.0%
Percent of incidents detected by the U.S. Computer Emergency Readiness Team for which targeted agencies are notified within 30 minutes (NPPD)	4.3	90.0%	92.0%	98.0%
Amount of dollar loss prevented by Secret Service cyber investigations (in millions) (USSS)	4.3	\$900	\$915	\$975
Number of law enforcement individuals trained in cybercrime and cyber forensics both domestically and overseas (USSS)	4.3	1,000	1,000	1,000
Percent of planned cyber security products and services transitioned to government, commercial, and open sources (S&T)	4.4	65%	80%	80%



## MISSION 5: STRENGTHEN NATIONAL PREPAREDNESS AND RESILIENCE

Despite ongoing vigilance and efforts to protect the United States and its citizens, major accidents, disruptions, and natural disasters, as well as deliberate attacks, will occur. The challenge is to build the capacity of American society to be resilient in the face of disruptions, disasters, and other crises. Our goals in this mission require us to: 1) enhance national preparedness; 2) mitigate hazards and vulnerabilities; 3) ensure effective emergency response; and 4) enable rapid recovery.

The 2014 Quadrennial Homeland Security Review reaffirms the Whole Community approach to national preparedness and resilience, which calls for the investment of everyone – not just the government – in preparedness efforts. Whole Community is a means by which emergency managers, organizational and community leaders, government officials, private and nonprofit sectors, faith-based and disability organizations, and the general public can collectively understand and assess the needs of their respective communities as well as determine the best ways to organize and strengthen their assets, capacities, and interests.

# DEPARTMENT MISSIONS AND GOALS

## MISSION PRIORITIES

The following Mission Priorities represent the highest priority efforts for the Department of Homeland Security within Mission 5. While the Department will continue to work on all of the mission goals and objectives laid out in the 2014 Quadrennial Homeland Security Review and the 2014-2018 Strategic Plan, these are the top areas of focus in terms of investment, strategic and operational planning, and stakeholder engagement, and will be addressed through actions undertaken in one or more of the following DHS foundational activities: Joint Requirements Council, joint operational plans and operations, enhanced budget and investment processes, and focused strategic and analytic efforts.

- **Prepare the Nation for those threats and hazards that pose the greatest risk to the security of the Nation** by building and sustaining capabilities in order to achieve the National Preparedness Goal.
- **Ensure effective, unified incident response operations.**

### GOAL 5.1: ENHANCE NATIONAL PREPAREDNESS

National preparedness underpins all efforts to safeguard and secure the Nation against those threats and hazards that pose the greatest risk. Presidential Policy Directive 8 calls for a National Preparedness Goal, which is “[a] secure and resilient Nation with the capabilities required across the Whole Community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.”

#### **We will pursue the following strategies to enhance national preparedness:**

*Empower individuals and communities to strengthen and sustain their own preparedness* by engaging public and community organizations through programs such as America’s Preparathon! to build a collective understanding of their risks, the resources available to assist their preparations, and their roles and responsibilities in the event of a disaster.

*Build and sustain core capabilities nationally to prevent, protect against, mitigate, respond to, and recover from all hazards* by conducting such activities as: 1) fostering capability development by providing tools and technical assistance; 2) providing planning and reach-back expertise; 3) using grant programs such as the State Homeland Security Grant Program and the Urban Area Security Initiative (which collectively provide funds to state, local, tribal, territorial, and regional government and port, transit, and nonprofit entities); and 4) promoting the use of the National Planning Frameworks. These activities support the Department’s intent to build and sustain a national integrated network of capabilities across all levels of government and to promote the involvement of the Whole Community in the



Nation's preparedness efforts.

*Assist federal entities in the establishment of effective continuity programs that are regularly updated, exercised, and improved by administering the National Exercise Program, the cornerstone of a collective effort to test, improve, and assess national preparedness.*

#### GOAL 5.2: MITIGATE HAZARDS AND VULNERABILITIES

DHS is uniquely positioned not only to support communities during a disaster, but also to enable partners to take steps that will decrease risk and mitigate future hazards before a disaster strikes. While risk cannot be totally eliminated, DHS can influence and support more positive outcomes in reducing risks. National risk management emphasizes focusing on those actions and interventions that reduce the greatest amount of strategic risk to the Nation.

##### **We will pursue the following strategies to mitigate hazards and vulnerabilities:**

*Promote public and private sector awareness and understanding of community-specific risks by providing credible and actionable data and tools to support risk-informed decision making and incentivizing and facilitating investments to manage current and future risk.*

*Reduce vulnerability through standards, regulation, resilient design, effective mitigation, and disaster risk reduction measures by encouraging appropriate land use and adoption of building codes, while also applying engineering and planning practices in conjunction with advanced technology tools.*

*Prevent maritime incidents by establishing, and ensuring compliance with standards and regulations by licensing U.S. mariners, conducting and sharing findings of casualty investigations, and providing grants and support for government and nongovernment boating safety efforts.*

#### GOAL 5.3: ENSURE EFFECTIVE EMERGENCY RESPONSE

DHS, primarily through the Federal Emergency Management Agency (FEMA) on land and the U.S. Coast Guard at sea, acts as the federal coordinator during disaster response, supporting state, local, tribal, territorial, and regional governments while working closely with nongovernmental organizations and the private sector to help leverage the resources they can bring to bear.

##### **We will pursue the following strategies to ensure effective emergency response:**

# DEPARTMENT MISSIONS AND GOALS

*Provide timely and accurate information* to individuals and communities to support public safety and inform appropriate actions by the public before, during, and after emergencies.

*Conduct effective, unified incident response operations* by following the National Response Framework, Second Edition; maximizing interagency coordination, information sharing, and preparation; and implementing initiatives to ensure a stable, flexible, and fully qualified disaster workforce.

*Provide timely and appropriate disaster assistance* through “survivor-centric” programs that support, streamline, and simplify the delivery of services for individuals and communities. DHS will strengthen capabilities and operationalize resource-sharing opportunities to achieve the greatest potential to change outcomes on the ground in catastrophic disasters.

*Ensure effective emergency communications* through the provision of technical communications capabilities enabling security, situational awareness, and operational decision making to manage emergencies under all circumstances.

## GOAL 5.4: ENABLE RAPID RECOVERY

DHS plays a key role in facilitating recovery following a disaster by supplementing communities' recovery core capabilities; promoting infrastructure resilience guidelines and use of standards; and encouraging the development of continuity plans for communities, government entities, and private-sector organizations. The devastating effects of recent disasters have highlighted the need to reform our national approach to long-term recovery. Communities devastated by a disaster, particularly large-scale events such as Hurricane Sandy, face complex and difficult challenges including restoring economic viability, rebuilding infrastructure and public services, and establishing resilience against future hazards.

### **We will pursue the following strategies to enable rapid recovery:**

*Ensure continuity and restoration of essential services and functions* by: 1) supplementing communities' recovery core capabilities; 2) encouraging the development of continuity plans for communities, government entities, and private-sector organizations; and 3) working to ensure continuity and rapid restoration of essential services.

*Support and enable communities to rebuild stronger, smarter, and safer* by following the National Disaster Recovery Framework and implementing programs that: 1) fund authorized federal disaster support activities; 2) support eligible reconstruction projects and disaster survivors; 3) provide subject matter experts to assist in planning and coordinating rebuilding efforts; and 4) focus on how best to restore, redevelop, and revitalize the health,

social, economic, natural, and environmental fabric of the community and build a more resilient nation.

#### HIGHLIGHTED PERFORMANCE MEASURES

The table below presents a subset of the DHS performance measures associated with gauging results for Mission 5. For more information on these measures, along with a more extensive list of measures associated with this mission, please see the FY 2013–2015 Annual Performance Report at <http://www.dhs.gov/xabout/budget/>

Mission 5: Strengthen National Preparedness and Resilience				
Highlighted Performance Measures	Goal Alignment	Planned Targets		
		FY 2014	FY 2015	FY 2018
Percent of households that participated in a preparedness exercise or drill at their workplace, school, home, or other community location in the past year (FEMA)	5.1	42%	44%	50%
Percent of communities in high earthquake, flood, and wind-prone areas adopting disaster-resistant building codes (FEMA)	5.2	57%	61%	64%
Reduction in the potential cost of natural disasters to communities and their citizens (in billions) (FEMA)	5.2	\$2.60	\$2.60	\$2.60
Percent of incident management and support actions necessary to stabilize an incident within 72 hours or by the agreed upon time (FEMA)	5.3	100%	100%	100%
Percent of orders for required life-sustaining commodities (meals, water, tarps, plastic sheeting, cots, blankets and generators) and key operational resources delivered by the agreed upon date (FEMA)	5.3	95%	95%	95%
Percent of people in imminent danger saved in the maritime environment (USCG)	5.3	100%	100%	100%
Percent of calls made by National Security/Emergency Preparedness users during emergency situations that DHS ensured were connected (NPPD)	5.3	100%	97%	98.5%
Percent of recovery services through Individual Assistance delivered to disaster survivors gauging the quality of program services, supporting infrastructure, and customer satisfaction following a disaster (FEMA)	5.4	92.0%	93.0%	96.0%
Percent of recovery services through Public Assistance delivered to communities gauging the quality of program services, supporting infrastructure, and customer satisfaction following a disaster (FEMA)	5.4	93.0%	93.0%	93.0%

# DEPARTMENT MISSIONS AND GOALS



Credit: U.S. Coast Guard

## MATURE AND STRENGTHEN HOMELAND SECURITY

The Nation's experiences in the years since September 11, 2001 highlight the importance of joining efforts across all levels of society and government into a common homeland security. In considering the evolution of the Department and the ever-changing environment in which it operates, we have identified several key, cross-cutting functional areas of focus for action within the Department that must be accomplished in order for it to successfully execute its core missions. These functions, and the critical activities associated with them, serve as the supporting foundation that underpins all homeland security missions.

These goals also support the Unity of Effort Initiative, which builds important linkages between the Department's planning, programming, budgeting, and execution processes, ensuring that the Department invests and operates in a cohesive, unified fashion, and makes decisions that are transparent and collaborative to drive the Secretary's strategic guidance to results.



## MISSION PRIORITIES

The following Mission Priorities represent the highest priority efforts for the Department of Homeland Security within Maturing and Strengthening Homeland Security. While the Department will continue to work on all of the mission goals and objectives laid out in the 2014 Quadrennial Homeland Security Review and the 2014-2018 Strategic Plan, these are the top areas of focus in terms of investment, strategic and operational planning, and stakeholder engagement, and will be addressed through actions undertaken in one or more of the following DHS foundational activities: Joint Requirements Council, joint operational plans and operations, enhanced budget and investment processes, and focused strategic and analytic efforts.

- **Enhance ability to analyze, fuse, and disseminate information and analysis** by improving integration of intelligence and operational activities — including screening and vetting practices and databases — investing in common enterprise solutions and services, and evolving toward real-time situational awareness, while protecting civil rights and civil liberties.
- **Enhance Unity of Effort** by strengthening forums for leadership decision-making, departmental management processes for investments, headquarters strategy, planning, and analytic capability, and coordinated operational planning.
- **Enhance employee morale** by recruiting, hiring, retain and developing a highly qualified, diverse, effective, mission-focused, and resilient workforce, and through providing expanded opportunities for professional growth and development.

### GOAL 1: INTEGRATE INTELLIGENCE, INFORMATION SHARING, AND OPERATIONS

Rapidly evolving threats and hazards demand that DHS and our partners continually enhance situational awareness. As noted earlier, DHS is committed to integrating critical data sources while maintaining and safeguarding a culture that preserves privacy and civil rights and civil liberties.

**We will pursue the following strategies to integrate intelligence, information sharing, and operations:**

*Enhance unity of regional operations coordination and planning* by partnering with and supporting the national network of fusion centers in the form of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding. DHS will also work to enhance intelligence enterprise support to Component and state, local, tribal, territorial and private sector homeland security missions by developing an integrated set of DHS intelligence enterprise priorities specific to collection and analysis and enhancing coordination among DHS head-

# DEPARTMENT MISSIONS AND GOALS

quarters, Component headquarters, and field elements.

*Share homeland security information and analysis, threats, and risks* by providing robust communications, coordination, information sharing, situational awareness capabilities, Department-level planning, and Department-level planning to homeland security partners.

*Integrate counterintelligence*, consistent with component and Departmental authorities, into all aspects of Department operations by utilizing the counterintelligence program management, counterintelligence analysis, and counterintelligence support and inquiries functions to safeguard homeland security-related national security information and other sensitive information.

*Establish a common security mindset with domestic and international partners*, through initiatives such as the DHS Common Operating Picture and the Homeland Security Information Network, which enable unity of effort with all homeland security partners, and through efforts to facilitate and integrate DHS's ability to share information with key foreign partners. Note that only trusted and vetted international partners receive access to properly screened sensitive information.

*Preserve civil rights, civil liberties, privacy, oversight, and transparency in the execution of homeland security activities* by creating appropriate policy as needed, advising Department leadership and personnel, assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information, and investigating and resolving any privacy, civil rights, or civil liberties complaints.

## GOAL 2: ENHANCE PARTNERSHIPS AND OUTREACH

Homeland security is achieved through a shared effort among all partners, from corporations to nonprofits and American families. Recent events, including the 2010 Deepwater Horizon oil spill and Hurricane Sandy, highlight the fundamentally important relationship that DHS must foster and sustain with the private sector as well as state, local, tribal, territorial, and international partners. In addition, rapidly evolving or emerging operating domains such as cyberspace and the Arctic are demanding new approaches and models for how DHS partners to achieve homeland security objectives.

**We will pursue the following strategies to enhance partnerships and outreach:**

*Promote regional response capacity and civil support* by coordinating and advancing federal interaction with state, local, tribal, and territorial governments and by pursuing the Whole Community approach to build and sustain national preparedness.

*Strengthen the ability of federal agencies to support homeland security missions by working with federal partners to ensure that Departmental roles, responsibilities, and interests are integrated with and incorporated into interagency activities.*

*Expand and extend governmental, nongovernmental, domestic, and international partnerships by building a Department-wide Community of Practice to synchronize the identification of potential partnership opportunities, develop a repository of partnerships and best practices, and serve as a consultative body to inform the exploration and formation of new public-private partnerships.*

*Further enhance the military-homeland security relationship by collaborating with the Department of Defense to pursue bilateral science and technology agreements; collaborate in information sharing and training; provide support for information systems Law Enforcement, and emergency and disaster response support; and develop international relationships.*

### GOAL 3: STRENGTHEN THE DHS INTERNATIONAL AFFAIRS ENTERPRISE IN SUPPORT OF HOMELAND SECURITY MISSIONS

DHS operates within a dynamic environment at home and abroad. The inherently transnational nature of homeland security missions necessitates a strong DHS international affairs enterprise that provides compatible visions of homeland security globally, a consistent and mutually beneficial cooperation with foreign partners, and an international footprint that maximizes mission effectiveness and return on investment.

**We will pursue the following strategies to strengthen the DHS international affairs enterprise in support of homeland security missions:**

*Establish strategic priorities for the Department's international affairs enterprise by engaging across Components in areas including policy analysis, cross-regional coordination, and management of international affairs issues, to establish a single, accepted view of DHS international operations and engagements. Implementation plans will be developed to responsibly document how DHS Components will implement these strategic priorities in a unified manner.*

*Establish coordination and communication mechanisms across the DHS international affairs enterprise to ensure national, Departmental and Component priorities are synchronized and DHS's international engagements are fully utilized to achieve common objectives.*



# DEPARTMENT MISSIONS AND GOALS

## GOAL 4: CONDUCT HOMELAND SECURITY RESEARCH AND DEVELOPMENT

Technology and homeland security are inextricably linked. A vast array of interdependent information technology networks, systems, services, and resources enable communication, facilitate travel, power our homes, run our economy and provide essential government services. These systems provide enormous benefits to our society and economy, but they also create new risks and vulnerabilities. DHS must endeavor to keep pace with technology and leverage research and development toward homeland security goals.

**We will pursue the following strategies to conduct homeland security research and development:**

*Employ scientific study to understand homeland security threats and vulnerabilities by pursuing a research and development strategy that is operationally focused, highly innovative, and founded on building partnerships among operators, scientists, and engineers, and by providing operational support, timely experiments, measurements, testing, evaluation, and analyses of homeland security significance.*

*Develop innovative approaches and effective solutions to mitigate threats and vulnerabilities by: 1) providing new capabilities through new technologies and operational process enhancements; 2) offering innovative systems-based solutions to complex problems; and 3) delivering the technical depth and reach to discover, adapt, and leverage scientific and engineering solutions developed by federal agencies and laboratories, state, local, and tribal governments, universities, and the private sector—across the United States and internationally.*



Credit: Science and Technology Directorate



*Leverage the depth of capacity in national labs, universities, and research centers by pursuing a mix of basic and applied research to deliver practical tools and analytic products that increase the effectiveness of components and save taxpayer dollars.*

#### GOAL 5: ENSURE READINESS OF FRONTLINE OPERATORS AND FIRST RESPONDERS

In an era of decreasing budgets and resources, partners across the Department must strive to find and develop innovative solutions for training, exercising, and evaluating capabilities. Achieving baseline proficiency and maintaining high levels of readiness in homeland security-related individual and collective skills and knowledge are critical to a unified partnership of law enforcement, first responders, and other front-line operators.

**We will pursue the following strategies to train and exercise frontline operators and first responders:**

*Support systems for training, exercising, and evaluating capabilities by pursuing integrated and cohesive cross-component training and evaluation.*

*Support law enforcement, first responder, and risk management training by providing coordinated, interoperable, and standardized law enforcement training to DHS and non-DHS federal agents/officers as well as to state, local, tribal and territorial and international entities.*

#### GOAL 6: STRENGTHEN SERVICE DELIVERY AND MANAGE DHS RESOURCES

To support priority security requirements in a sustainable way, we must become more efficient and effective across a large and federated structure. As a Department, we must eliminate duplicative processes, develop common platforms, and purchase single solutions. In addition, the safety and security of our country can only be achieved through the hard work and dedication of our employees, with a diverse array of backgrounds, experiences, skills, and ideas. Our workforce serves as the foundation to ensure continued growth of our collective ability to prevent and respond to the threats facing the nation.

**We will pursue the following strategies to strengthen service delivery and manage DHS resources:**

*Recruit, hire, retain, and develop a highly qualified, diverse, effective, mission-focused, and resilient workforce by implementing programs and resources that focus on four key objectives: 1) building an effective, mission-focused, diverse, and inspiring cadre of leaders; 2) recruiting a highly qualified and diverse workforce; 3) retaining an engaged workforce; and 4) solidifying a DHS culture of mission performance, adaptability, accountability, equity, and results.*

# DEPARTMENT MISSIONS AND GOALS



Credit: Transportation Security Administration

*Manage the integrated investment life cycle to ensure that strategic and analytically based decisions optimize mission performance by integrating performance with program plans and budgets that are well justified and balanced to support DHS priorities.*

*Manage and optimize financial resources, property/assets, procurements, security, and DHS IT by: 1) strengthening department service delivery in partnership with all components through integration teams to achieve affordable readiness; 2) pursuing strategic sourcing, small business utilization, and acquisition workforce management; and 3) maintaining a Department-wide IT infrastructure that is reliable, scalable, flexible, maintainable, accessible, secure, meets users'*

needs, and ensures operational excellence—from the workstation to the data center to the mission application.

*Establish and execute a comprehensive and coordinated DHS health and medical system by providing medical guidance and Department-wide solutions to mitigate adverse health impacts and work-related health risks to support DHS employees and by embedding senior medical advisors with select operational components to develop and implement policies and procedures to improve force health protection, emergency medical services, global health security, and occupational health and wellness.*

## HIGHLIGHTED PERFORMANCE MEASURES

The table below presents a subset of the DHS performance measures associated with gauging results for the Mature and Strengthen area. For more information on these measures, along with a more extensive list of measures associated with this area, please see the FY 2013–2015 Annual Performance Report at [http://www.dhs.gov/xabout/budget/editorial\\_0430.shtm](http://www.dhs.gov/xabout/budget/editorial_0430.shtm).

Mature and Strengthen the Department				
Highlighted Performance Measures	Goal Alignment	Planned Targets		
		FY 2014	FY 2015	FY 2018
Percent of initial breaking homeland security blast calls initiated between the National Operations Center and designated homeland security partners within targeted timeframes (AO - OPS)	MS1	98%	98%	98%
Percent of Homeland Security Advanced Research Projects Agency (HSARPA) program milestones that are met, as established in the fiscal year's budget execution plan (S&T)	MS4	75%	75%	75%
Percent of Partner Organizations that agree the FLETC training programs address the right skills (e.g., critical knowledge, key skills and techniques, attitudes/behaviors) needed for their officers/agents to perform their law enforcement duties (FLETC)	MS5	97%	97%	97%
Percent of veteran hires among total DHS hires in each fiscal year (DMO - CHCO)	MS6	25%	25%	25%
Percent of environmentally preferable and sustainable purchasing actions (DMO - CPO)	MS6	95%	95%	95%
Percent of Equal Employment Opportunity complaints timely adjudicated (DMO - CRCL)	MS6	40%	45%	60%
Percent reduction in scope 1 & 2 greenhouse gas emissions (DMO - CRSO)	MS6	5%	7%	19%

# APPENDIX A

## APPENDIX A: MISSION PROGRAMS BY GOAL

The table below identifies the DHS programs that contribute to each goal. A mission program is defined as an organized set of activities acting together to accomplish high-level outcomes. Mission programs are the operational processes, skills, technology, human capital, and other resources leveraged to achieve Department missions, goal, and sub-goals. Mission programs are those programs that reside in the Future Years Homeland Security (FYHSP) system.

### Mission 1

#### Goal 1.1

##### AO

- Analysis and Operations

##### CBP

- Integrated Operations
- Intelligence and Targeting
- Management and Administration
- Securing America's Borders
- Securing and Expediting Trade
- Securing and Expediting Travel

##### FLETC

- Law Enforcement Training

##### ICE

- Automation Modernization
- Homeland Security Investigations (HSI)

##### ST

- Research, Development, and Innovation

##### TSA

- In Flight Security
- Intermodal Assessments and Enforcement

##### ment

- Intermodal Screening Operations
- Management and Administration

##### USCG

- Cross-Cutting Capital Investments and Maintenance
- Defense Operations
- Maritime Prevention
- Maritime Security Operations
- Mission Support

#### Goal 1.2

##### AO

- Analysis and Operations

##### CBP

- Integrated Operations
- Intelligence and Targeting
- Management and Administration

##### DNDO

- Domestic Rad/Nuc Detection, Forensics and Prevention Capability

##### NPPD

- Infrastructure Protection

##### OHA

- Health Threats Resilience

##### ST

- Research, Development, and Innovation

##### TSA

- Intermodal Assessments and Enforcement

##### USCG

- Cross-Cutting Capital Investments and Maintenance
- Maritime Security Operations
- Mission Support



### Goal 1.3

#### AO

- Analysis and Operations

#### CBP

- Integrated Operations
- Intelligence and Targeting
- Management and Administration
- Securing America's Borders

#### FLETC

- Law Enforcement Training

#### NPPD

- Federal Protective Service
- Infrastructure Protection

#### USCG

- Cross-Cutting Capital Investments and Maintenance
- Defense Operations
- Maritime Prevention
- Maritime Security Operations
- Mission Support

#### USSS

- Criminal Investigations
- Information Integration and Technology Transformation
- Management and Administration
- Protection
- Protective Intelligence
- Rowley Training Center

### Mission 2

#### Goal 2.1

#### AO

- Analysis and Operations

#### CBP

- Integrated Operations
- Intelligence and Targeting
- Management and Administration
- Securing America's Borders
- Securing and Expediting Trade

- Securing and Expediting Travel

#### FLETC

- Law Enforcement Training

#### NPPD

- Office of Biometric Identity Management

#### ST

- Research, Development, and Innovation

#### USCG

- Cross-Cutting Capital Investments and Maintenance
- Defense Operations
- Maritime Law Enforcement
- Mission Support

#### Goal 2.2

#### CBP

- Integrated Operations
- Intelligence and Targeting
- Management and Administration
- Securing and Expediting Trade
- Securing and Expediting Travel

#### FLETC

- Law Enforcement Training

#### ICE

- Homeland Security Investigations (HSI)
- Management and Administration

#### ST

- Research, Development, and Innovation

#### TSA

- Intermodal Assessments and Enforcement

#### USCG

- Cross-Cutting Capital Investments and Maintenance

# APPENDIX A

- Marine Transportation System Management
- Maritime Law Enforcement
- Maritime Prevention
- Mission Support

## Goal 2.3

### CBP

- Intelligence and Targeting
- Securing America's Borders

### FLETC

- Law Enforcement Training

### ICE

- Automation Modernization
- Homeland Security Investigations (HSI)

### ST

- Research, Development, and Innovation

### USCG

- Cross-Cutting Capital Investments and Maintenance
- Defense Operations
- Maritime Law Enforcement
- Mission Support

## Mission 3

### Goal 3.1

#### ICE

- Homeland Security Investigations (HSI)

#### NPPD

- Office of Biometric Identity Management

#### USCIS

- Adjudication Services
- Citizenship
- Crosscutting Investments
- Immigration Status Verification
- Information and Customer Service
- Management and Administration

## Goal 3.2

### CBP

- Integrated Operations
- Intelligence and Targeting
- Management and Administration
- Securing America's Borders

### FLETC

- Law Enforcement Training

### ICE

- Automation Modernization
- Construction
- Enforcement and Removal Operations (ERO)
- Homeland Security Investigations (HSI)
- Management and Administration

### NPPD

- Office of Biometric Identity Management

### ST

- Research, Development, and Innovation

### USCG

- Cross-Cutting Capital Investments and Maintenance
- Maritime Law Enforcement
- Mission Support

### USCIS

- Crosscutting Investments
- Immigration Security and Integrity
- Immigration Status Verification
- Management and Administration

## Mission 4

### Goal 4.1

#### AO

- Analysis and Operations

#### FLETC

- Law Enforcement Training

#### ICE

- Homeland Security Investigations (HSI)

#### NPPD

- Cybersecurity and Communications
- Federal Protective Service
- Infrastructure Protection
- Office of Cyber and Infrastructure Analysis

#### Goal 4.2

##### NPPD

- Cybersecurity and Communications

#### Goal 4.3

##### FLETC

- Law Enforcement Training

##### NPPD

- Cybersecurity and Communications

##### ST

- Research, Development, and Innovation

##### USSS

- Criminal Investigations
- Information Integration and Technology Transformation
- Management and Administration
- Rowley Training Center

#### Goal 4.4

##### FLETC

- Law Enforcement Training

##### NPPD

- Cybersecurity and Communications

##### ST

- Research, Development, and Innovation

#### Mission 5

#### Goal 5.1

##### AO

- Analysis and Operations

#### CBP

- Integrated Operations

##### FEMA

- Management and Administration
- Mission Program Support
- Preparedness
- Protection
- Recovery
- Response

##### FLETC

- Law Enforcement Training

##### OHA

- Health Threats Resilience
- Workforce Health and Medical Support

##### ST

- Research, Development, and Innovation

##### USCG

- Cross-Cutting Capital Investments and Maintenance
- Maritime Response
- Mission Support

#### Goal 5.2

##### FEMA

- Management and Administration
- Mission Program Support
- Mitigation

##### FLETC

- Law Enforcement Training

##### ICE

- Homeland Security Investigations (HSI)
- Management and Administration

##### ST

- Acquisition and Operations Support

##### USCG

- Cross-Cutting Capital Investments and

# APPENDIX A

## Maintenance

- Marine Transportation System Management
- Maritime Prevention
- Mission Support

## Goal 5.3

### AO

- Analysis and Operations

### CBP

- Integrated Operations
- Securing America's Borders

### FEMA

- Management and Administration
- Mission Program Support
- Preparedness
- Protection
- Recovery
- Response

### FLETC

- Law Enforcement Training

### ICE

- Homeland Security Investigations (HSI)
- Management and Administration

### NPPD

- Cybersecurity and Communications

### OHA

- Workforce Health and Medical Support

### ST

- Research, Development, and Innovation

### USCG

- Cross-Cutting Capital Investments and Maintenance
- Maritime Response
- Mission Support

## Goal 5.4

### AO

- Analysis and Operations

## CBP

- Integrated Operations

## FEMA

- Management and Administration
- Mission Program Support
- Mitigation
- Protection
- Recovery
- Response

## FLETC

- Law Enforcement Training

## ST

- Management and Administration
- Research, Development, and Innovation

## USCG

- Cross-Cutting Capital Investments and Maintenance
- Maritime Response
- Mission Support

## Maturing and Strengthening

### Goal 1

### AO

- Analysis and Operations

### CBP

- Management and Administration

### DMO

- Mission Support - Office of the Secretary and Executive Management
- Mission Support - Under Secretary for Management

### FEMA

- Management and Administration

### ICE

- Homeland Security Investigations (HSI)
- Management and Administration

### OHA

- Health Threats Resilience



ST

- Research, Development, and Innovation

USCG

- Mission Support

*Goal 2*

AO

- Analysis and Operations

DMO

- Mission Support - Office of the Secretary and Executive Management

OHA

- Health Threats Resilience

ST

- Acquisition and Operations Support

USCG

- Mission Support

USSS

- Criminal Investigations

*Goal 3*

DMO

- Mission Support - Office of the Secretary and Executive Management

ST

- Acquisition and Operations Support

USCG

- Mission Support

*Goal 4*

ST

- Laboratory Facilities
- University Programs

USCG

- Mission Support

*Goal 5*

DMO

- Mission Support - Office of the Secretary and Executive Management

FLETC

- Accreditation
- Law Enforcement Training

OHA

- Workforce Health and Medical Support

ST

- Acquisition and Operations Support

*Goal 6*

AO

- Analysis and Operations

CBP

- Integrated Operations
- Management and Administration

DMO

- Mission Support - Office of the Secretary and Executive Management
- Management and Administration - Office of the Secretary and Executive Management
- Management and Administration - Under Secretary for Management

DNDO

- Management and Administration

FEMA

- Management and Administration

FLETC

- Management and Administration

ICE

- Management and Administration

IG

- Audits, Inspections, and Investigations
- Management and Administration

# APPENDIX A

## NPPD

- Management and Administration

## OHA

- Management and Administration
- Workforce Health and Medical Support

## ST

- Management and Administration
- University Programs

## TSA

- Management and Administration

## USCG

- Management and Administration
- Mission Support

## USCIS

- Adjudication Services
- Management and Administration

## USSS

- Management and Administration

## ACRONYM LIST

AO	Analysis and Operations
CBP	U.S. Customs and Border Protection
DMO	Department Management and Operations
DNDO	Domestic Nuclear Detection Office
FEMA	Federal Emergency Management Agency
FLETC	Federal Law Enforcement Training Centers
ICE	Immigration and Customs Enforcement
IG	Inspector General
NPPD	National Protection and Programs Directorate
OHA	Office of Health Affairs
ST	Science and Technology
TSA	Transportation Security Administration
USCIS	United States Citizenship and Immigration Services
USCG	United States Coast Guard
USSS	United States Secret Service

# APPENDIX B

## APPENDIX B: UNITY OF EFFORT INITIATIVE

The strategic decisions of the Department's senior leadership are only as good as the processes that support and give effect to those decisions through investments and in the conduct of operations. Historically, DHS has generally developed and executed Component-centric requirements, which has resulted in inefficient use of limited resources. Much work has been done to date in the areas of joint requirements analysis, program and budget review, and acquisition oversight, including an effort over the past four years by the DHS Management Directorate to improve the Department's overall acquisitions process, reforming even the earliest phase of the investment life cycle where requirements are first conceived and developed. To make further progress, the Department will make use of existing structures and create new capability, where needed, as revealed by the recent Integrated Investment Life Cycle Management pilot study. That effort tested process linkages and underscored the need to further strengthen all elements of the process, particularly the up-front development of strategy, planning, and joint requirements so that these elements are developed based on DHS-wide missions and functions, rather than focusing on those of an individual Component.

The Department is capitalizing on these previous efforts and broadening them in the Unity of Effort Initiative. This effort focuses on improving the DHS planning, programming, budgeting, and execution processes through strengthened Departmental structures and increased capability. In making these changes, the Department will have better traceability between strategic objectives, budgeting, acquisition decisions, operational plans, and mission execution to improve Departmental cohesiveness and operational effectiveness—realizing the vision of a true “guidance to results” framework for DHS. Individual components have taken this commitment to heart, as evidenced, for example, by the U.S. Coast Guard Unity of Effort Management Imperative.

Specifically, the Department is prioritizing its efforts on the following focus areas that are intended to build organizational capacity to develop action plans and implement change:

**Departmental Leadership Forums:** The Secretary (Senior Leaders Council) and Deputy Secretary (Deputy's Management Action Group) chair twice-monthly forums of the DHS Components and select headquarters counterparts, gathering in an environment of trust, and openly placing on the table issues, arguments, and disagreements concerning the Department's most challenging issues. These meetings, convened to discuss issues of overall policy, strategy, operations and Departmental guidance, are already moving forward specific initiatives in joint requirements development, program and budget review, acquisition reform, operational planning, and joint operations.



**Departmental Management Processes for Investments:** The DHS Chief Financial Officer is strengthening and enhancing the Department's programming and budgeting process by incorporating the results of strategic analysis and joint requirements planning into portfolios for review by cross-component issue teams. Substantive, large-scale alternative choices have been presented to the Deputies Management Action Group as part of the annual budget development. This review process also includes the Department's existing programmatic and budgetary structure, not just new investments, as well as the ability for DHS to project the impact of current decisions on resource issues such as staffing, capital acquisitions, operations and maintenance, and similar issues that impact the Department's future ability to fulfill its mission responsibilities.

In addition, the Department has established a joint requirements council to lead an enhanced DHS joint requirements process. This new council has already begun to identify priority gaps and overlaps in Departmental capability needs, and will use DHS's analytic capabilities to develop feasible technical alternatives to meet capability needs, and provide them, along with recommendations for creation of joint programs and joint acquisitions to meet Departmental mission needs, where appropriate, for senior leader decision.

Finally, Under Secretary of Management has conducted a full review of the Department's acquisition oversight framework and is taking action to update the processes, ultimately resulting in a transparent, comprehensive continuum of activities that link and integrate Departmental strategy and planning, development of joint requirements, programming and budgeting decisions, capital investment planning, and the effective and efficient execution of major acquisitions and programs.

**DHS Headquarters Strategy, Planning, and Analytical Capability:** The Department has taken action to focus its Departmental level strategy, planning, and analytical capability to more robustly understand and coordinate with DHS Component level functions to support more effective DHS-wide operations. This enhanced capability better supports Secretary in executing the responsibility to understand from a Departmental perspective how the activities, operations, and programs of each individual Component fit together in order to best meet Departmental mission responsibilities in a constrained resource environment. The goal in focusing the collective DHS Headquarters capability, which will harness a number of existing analytic cells throughout DHS, is not to eliminate the need for Component-level planning or analysis. To the contrary, this new, focused DHS Headquarters capability will work together with the planning and analytical organizations within each Component to develop a comprehensive picture of the Department's mission responsibilities and functional capabilities, and to identify points of friction or gaps, thus framing the corresponding choices

## APPENDIX B

that must be made. This capability will be integrated into, not created and employed in isolation from, existing Departmental functions that are critical to day-to-day mission execution and mission support activities.

**Departmental Processes for Enhancing Coordinated Operations:** The strategic decisions of the Department's senior leadership and the investments our Department makes in current and future capabilities will only be effective if cross-department operations are planned and executed in a coordinated fashion. Many DHS operations are conducted solely by a single Component, although successful examples of joint operational activities exist in seaports such as Charleston, SC, Miami, FL, San Diego, CA, and Seattle, WA, and through organizations chartered under the National Interdiction Command and Control Plan such as Joint Interagency Task Force-South in Key West, FL, the El Paso Intelligence Center in El Paso, TX, and the Air and Marine Operations Center in Riverside, CA.

Supporting this objective, the Department is exploring, concurrent with the development of joint operational plans, additional strategic alternatives for future coordinated operations. Enhancing the effectiveness and unity of DHS operations to better fulfill the Department's mission responsibilities is the primary reason for making these important changes, which represent a degree of departure from current DHS and Component level approaches to management and operations. But in adding structure and transparency, combined with collaborative, forthright senior leader engagement the Department will build together a stronger, more unified, and enduring DHS.

### END EFFECT – WHAT SUCCESS LOOKS LIKE

Unity of Effort is the state of integrating DHS organizations: *the whole is so much more powerful than the sum of the parts*. This will be achieved through integrated governance, strategy, processes, analysis, and culture.

### INTEGRATED GOVERNANCE

Managing and implementing key enterprise decisions. Key success factors:

- **Leadership accountability;** roles and responsibilities are clear, understood, and effective
- **Delegations of authorities** are clear, understood and effective
- **Priorities** support DHS enterprise
- **Data driven, transparent, objective** decision making
- Executive decisions are **communicated and implemented**
- **Coordinated, collaborative management and execution**

## INTEGRATED STRATEGY

Defining and implementing DHS strategic intent. Key success factors:

- Strategic development process is **documented, transparent, timely, synchronized, repeatable, and balanced**
- **Authorities, roles, and responsibilities** are clearly articulated and documented
- **Strategy drives resource planning (PPB&E ) and joint operational planning**, and aligns with timelines
- **Planning emphasizes** long-term (e.g., QHSR) and mid-term (e.g., FYHSP) **strategic intent**
- **Implementation** aligns with strategic intent
- Feedback loop rapidly **incorporates lessons learned** (e.g., capability gaps) back into planning cycle

## INTEGRATED PROCESSES

Synchronizing DHS processes to provide collaborative and efficient delivery of services. Key success factors:

- Processes are **documented, transparent, timely, synchronized, stable, and repeatable**
- Process methodology is **agile and responsive**
- Processes include **quantitative measures**
- **Incorporates strategy**, capabilities and requirements, PPB&E, and acquisitions
- Feedback loop rapidly **incorporates lessons learned** back into process

## INTEGRATED ANALYSIS

Integrating accurate and relevant information to inform DHS decision makers. Key success factors:

- Analysis is **documented, transparent, synchronized, and repeatable**
- Analysis is **timely for decision making**
- Measures are **quantifiable, repeatable, and actionable**
- Strategic analysis and lessons learned **inform operational planning**
- Operational analysis **emphasizes capabilities** and informs **joint requirement development**

## INTEGRATED CULTURE

Supporting DHS common goals. Key success factors:

- Component priorities **support overarching DHS missions**
- **Responsive** to homeland security enterprise demands
- **Commitment to collaborate** and coordinate capabilities, assets and other resources

# APPENDIX C

## APPENDIX C: AGENCY PRIORITY GOALS

During FY 2014–2015, the Department will continue to pursue the priorities expressed in the FY 2012–2014 Agency Priority Goals but is maturing the goals to drive results in areas identified as Administration priorities. The following tables summarize the FY 2014–2015 Agency Priority Goals. Results for these goals will be available quarterly on [www.performance.gov](http://www.performance.gov).

<b><i>Agency Priority Goal 1: Strengthen Aviation Security Counterterrorism Capabilities and Improve the Passenger Experience by Using Intelligence Driven Information and Risk-Based Decisions</i></b>	
<b>Goal Statement</b>	By September 30, 2015, TSA will expand the use of risk-informed security initiatives to increase the percentage of travelers eligible for expedited screening at airports to 50 percent and enhance the passenger experience.
<b>Overview</b>	<p>TSA performs and oversees security operations at the Nation's airports, screening more than 650 million passengers annually, to ensure the freedom of movement of people and commerce. In an effort to strengthen aviation security while enhancing the passenger experience, TSA is focusing on risk-informed, intelligence-driven security procedures and enhancing its use of technology. Since 2011, the Agency has implemented several risk-informed initiatives including implementation of the TSA Pre✓™ expedited screening program; the nationwide implementation of modified screening protocols for passengers 12 and younger, passengers 75 and over, and active-duty service members; expediting physical screening of Veterans on chartered Honor Flights; and providing modified screening to Wounded Warriors. A number of initiatives will further enable TSA to reach its goal of expanding expedited screening for known populations in order to focus on those that are unknown including development and deployment of the TSA Pre✓™ Application and TSA Risk Assessment programs; expansion of TSA Pre✓™ participation to international air carriers; continued expansion of the Known Crewmember program; and developing operational policies, procedures, and other activities such as the evolution of checkpoint screening technologies to support deployment of Risk Assessments that will grow the volume of passengers eligible for expedited screening.</p> <p>As of December 2013, on a weekly basis, more than 32% of passengers receive some form of expedited screening, and TSA expects to continue to increase that number. While driving the growth of eligible populations is key to the initiative's long-term success, TSA faces challenges in aligning, planning, and executing activities for incorporating these various populations. The success of achieving TSA's risk-informed security milestones is in many ways reliant upon external and internal partners that TSA continues to work with to mitigate these challenges.</p>



**Agency Priority Goal 2: Enforce and Administer Our Immigration Laws Through Prioritized Detention**

<b>Goal Statement</b>	By September 30, 2015, ICE will increase criminal alien removals, as a percentage of total removals, by 5 percent.
<b>Overview</b>	<p>U.S. Immigration and Customs Enforcement (ICE) is committed to identifying, arresting, detaining, prosecuting, and removing aliens who present a danger to national security or are a risk to public safety, as well as those who otherwise undermine the integrity of our immigration laws and border control efforts. These include, but are not limited to aliens engaged in or suspected of terrorism or espionage; violent criminals, felons, and repeat offenders; and organized criminal gang members. Also critical to ICE enforcement priorities are recent illegal border crossers.</p> <p>This goal is a continuation of the effort that began in FY 2012 to increase efficiencies in the process of detaining and removing illegal aliens. The next two years will be to showcase ICE's abilities to remove criminal aliens from the United States. These efforts include identifying and apprehending at-large criminal aliens and expanding coverage in jails and prisons in order to identify and process removable incarcerated foreign-born detainees. Through the use of Secure Communities, ICE continues to work with the Federal Bureau of Investigation (FBI) to identify criminal aliens who have been booked into custody, without imposing new or additional requirements on state and local law enforcement. This is accomplished by checking fingerprints submitted to the FBI by the arresting law enforcement agency against the DHS's immigration database to determine if the suspect has a criminal or immigration history, and/or is otherwise removable from the United States due to a criminal conviction.</p> <p>ICE has expanded the exercise of prosecutorial discretion through initiatives such as the case-by-case review, which improves efficiencies by identifying and eliminating low-priority cases clogging the immigration system. The use of prosecutorial discretion also allows ICE to prioritize the use of its enforcement personnel, detention space, and removal assets to ensure that the aliens it removes represent, as much as reasonably possible, ICE enforcement priorities, namely the promotion of national security, border security, public safety and the integrity of the immigration system.</p>

**Agency Priority Goal 3: Ensure Resilience to Disasters by Strengthening Disaster Preparedness and Response Capabilities**

<b>Goal Statement</b>	By September 30, 2015, 39 states and territories will demonstrate improvement in achieving their core capability targets established through their Threat and Hazard Identification and Risk Assessment (THIRA).
<b>Overview</b>	<p>To enhance national preparedness and resilience, FEMA established THIRA to provide a common approach for identifying and assessing risks and documenting their associated impacts. Developing an understanding of risks from natural, technological, and human-caused threats and hazards allows a community to make informed decisions about how to manage risk and develop needed capabilities.</p> <p>In addition, states and territories assess their current capability and set targets for improvement for preventing, protecting against, mitigating, responding to, and recovering from these threats and hazards. FEMA expects states and territories to mature and demonstrate improvement in achieving their capability targets over the next 2 years through their THIRAs.</p>

## SECURITY AND TRAVEL FACILITATION

The Department of Homeland Security (DHS) maintains high levels of security, while facilitating domestic and international travel in the land, air, and sea environments. The Transportation Security Administration (TSA) is charged with protecting the nation's transportation systems, and U.S. Customs and Border Protection (CBP) is responsible for ensuring U.S. border security; at the same time, both agency missions seek to ensure the facilitation of legitimate travel. Accordingly, the mission of DHS as it relates to security and travel facilitation, has a direct and significant impact on our national security and economic prosperity. The travel environment also presents a unique space in which DHS often collaborates with other public and private sector stakeholders to better secure and serve the public; and has a wide array of interested and vocal stakeholders including travelers, industry associations, local partners, and Congress. Ultimately, DHS's goal is to provide seamless entry and exit screening, vetting, and verification processes using the most advanced technologies, such as biometrics, while ensuring our national security and the safety of the traveling public.

Key challenges in the security and travel facilitation space include a dynamic threat environment — including efforts by terrorists to evade aviation and border security; increases in the number of individuals requiring access or credentials to critical transportation sectors; and a continuing increase in the number of lawful travelers within and to the United States. To meet these challenges, DHS must continue to evolve its security and travel facilitation posture through: investments in DHS's **targeting, screening, and vetting infrastructure**; efforts to **identify and interdict potential threats at the earliest possible moment** and prior to departure to or encounter in the United States; the continued development of **business transformation initiatives** that optimize the use of resources; **joint initiatives** between CBP and TSA for both security and facilitation; and continued advancement of the use of **biometrics** throughout the travel continuum for better security and facilitation.

[Return to Top](#)

## **IMMIGRATION AREAS OF FOCUS**

- The administration and enforcement of our immigration laws will continue to be a highly controversial and carefully scrutinized element of the DHS mission. While border management and security often receive the greatest political scrutiny, the scope of DHS's work covers all aspects of immigration law from regulating the flow of people across our borders, to providing humanitarian protections, to removing individuals, to adjudicating immigration benefits, and to naturalizing new citizens. Managing these complex, and sometimes competing interests requires significant coordination between headquarters (PLCY, OGC, PRIV, CRCL) and the three main immigration agencies (USCIS, CBP, ICE), and significant unity of effort initiatives.
- Critical to the successful development of immigration policy is a broad view of the impact immigration plays in our society and the economy (diversity, workforce, entrepreneurship, innovation) in terms of both costs and benefits. Equally critical is an understanding of the limitations of immigration law – for example, in addressing exploitation of vulnerable populations by human smugglers and traffickers and individuals who may pose risks to National security.
- The most pressing immigration issues remain immigration reform and addressing the undocumented population of close to 11 million people. Key reform areas of focus are:
  - Legal immigration demand far exceeds supplies of available visas.
  - High levels of congressional and public scrutiny may impede reform efforts and particularly pathways to addressing the undocumented migrant population.
  - Addressing the key factors driving human smuggling, trafficking, and other criminal enterprises.
- Potential courses of action to address this issue include legislative and regulatory reform, policy review and reform, improved operational and technological efficiencies, and a unified effort to communicate enforcement of laws that support national security, public safety, border management and the integrity of a thriving immigration system.

[Return to Top](#)

## **PERSISTENT THREATS TO TRANSPORTATION AND SECURITY**

- The U.S. transportation sector is an enduring terrorist target based on sustained terrorist interest in the sector and recent international attacks on aviation and mass transit. In the first half of 2016, there were 13 attacks against civil aviation abroad, a 117 percent increase from the same time period in 2015. During this same timeframe, there were 30 attacks against mass transit assets worldwide.
- Homegrown Violent Extremists inspired by foreign terrorists pose the most likely domestic transportation threat and can use small arms and rudimentary explosive devices against airports, surface, and maritime transportation with little to no warning.
- The Department of Homeland Security (DHS) works with federal, state, local, tribal, territorial, private sector, and international partners to protect and deny terrorists access to critical transportation infrastructure. DHS continues to prioritize preventing terrorists and radicalized individuals from traveling to the U.S. to launch attacks.
- There are several significant trends with respect to transportation threats:
  - Multiple terrorist groups recently conducted, planned, or attempted international aviation sector attacks and still prioritize targeting of aviation and its infrastructure.
  - Trusted transportation insiders facilitated several recent attacks on international aviation and associated infrastructure, posing an enduring concern regarding insider threats.
  - Terrorist organizations attacked public portions of the airport to cause mass casualties during recent attacks in Brussels, Belgium and Istanbul, Turkey.
  - Terrorist networks conducted recent attacks against in-flight aviation internationally including the destruction of a Metrojet Airlines flight over Egypt's Sinai Peninsula and detonation of an explosive device aboard a Daallo Airlines flight over Somalia.
  - Terrorist groups understand the economic consequences of aviation attacks, including negative impacts on tourism industries following the recent aviation-focused attacks.
  - Terrorist groups and radicalized individuals continue to engage in international attacks against surface transportation including passenger and freight rail and mass transit passengers.
- Aviation passenger and cargo operations are closed systems with interdependent security protocols, requiring each element of the security regime to perform its function to safeguard the sector. Risks to the sector include domestic or international partners failing to follow protocols and transportation insiders facilitating terrorist attacks.
- The public portions of airports and surface transportation including rail, mass transit, and highway systems do not have intensive security regimes and are optimized to facilitate the efficient flow of people and goods. These systems are more vulnerable to attack than aviation.



- DHS uses several approaches to mitigate transportation threats and applies an intelligence-driven risk-based security approach to safeguard transportation systems tailored to each specific threat. Responses may include:
  - Stakeholder information sharing initiatives.
  - Changes to security operations.
  - Enhancements to training.
  - Deployment of law enforcement personnel.
  - Issuing regulatory requirements for enhanced security measures.
  - Foreign partner assistance.
  - Providing security operations with improved technology to prevent and mitigate terrorist attacks.

[Return to Top](#)

## CYBERSECURITY RESPONSIBILITIES AND AUTHORITIES

- Cyber threats continue to grow and evolve at a rapid pace. Such threats are seen across Government networks and all U.S. critical infrastructure sectors, including the Financial Services, Energy, Transportation, Emergency Services, Information Technology, Communications, and Healthcare and Public Health sectors. Potential impacts from cyber incidents include data corruption, data theft, and physical consequences.
- DHS has broad cybersecurity responsibilities and authorities, including responsibility to protect the Federal civilian government, enhance the security and resilience of critical infrastructure, investigate cyber crimes, respond to incidents, and improve the overall cyber ecosystem. DHS is directed, in multiple laws and executive orders (EOs), to conduct these missions in a manner that respects privacy and civil liberties.
- DHS cybersecurity programmatic efforts can be generally grouped into the following activities:
  - Secure federal information systems;
  - Push the private sector to adopt best practices;
  - Respond effectively to cyber incidents;
  - Share timely and actionable cybersecurity information;
  - Pursue, disrupt, and deter cybercrimes;
  - Enhance the security and resilience of technology products; and
  - Improve the cyber ecosystem through research and development, international engagement, education and training.
- The *2014 Quadrennial Homeland Security Review*<sup>1</sup> identifies “Safeguarding and Securing Cyberspace” as one of five core DHS mission areas. The Office of Policy (PLCY) is responsible for developing DHS-wide strategic approaches across the cybersecurity mission.

[Return to Top](#)

---

<sup>1</sup> <https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>

## IMMIGRATION AND CUSTOMS ENFORCEMENT AREAS OF FOCUS: SMUGGLING NETWORKS EXPLOITING OUR BORDERS

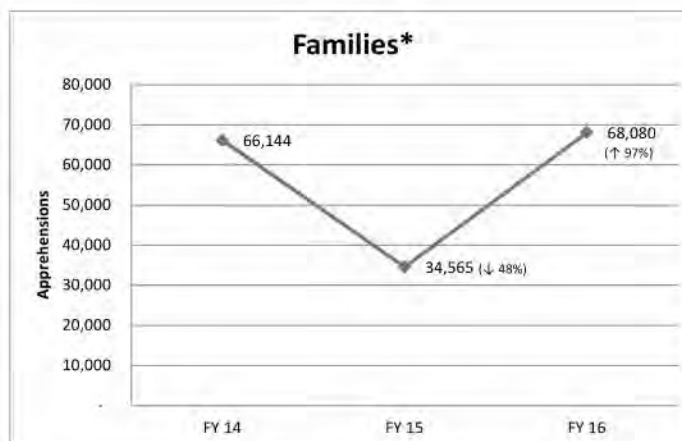
- U.S. Immigration and Customs Enforcement's (ICE) strategic goals include prioritizing efforts to deter, interdict, and dismantle smuggling networks which exploit our borders to market their illicit activities, to include heroin and fentanyl smuggling. ICE will focus on human smuggling networks and preventing illicit travel into the United States, and prioritize vulnerable populations, such as unaccompanied minors and families.
- There are numerous smuggling networks motivated by financial gain, which vary in size and complexity. Some groups are comprised of family members or close associates, while others—including those smuggling non-Western Hemisphere migrants—are more complex because the smuggling involves more complicated international planning and logistics between source, transit, and destination countries. Regardless of origin, immigrants reaching the Western Hemisphere use the distributed and non-hierarchical smuggling networks through all transit countries.

### *Drug Smuggling*

- The nation has seen a tremendous increase in the trafficking and use of fentanyl, fentanyl analogues, and other dangerous synthetic opioids. Drug trafficking organizations are realizing the profit margins on fentanyl-related compounds and have begun distributing increased amounts of these compounds in lieu of heroin. In 2016, overdose incidents spiked in multiple states and have been attributed to the market infiltration of the fentanyl-related compounds. Due to their addictive nature and demand for these compounds, a myriad of international drug trafficking organizations are competing for the U.S. domestic market. As part of the increase in investigations of these drug trafficking organizations, ICE Homeland Security Investigations (HSI) has engaged in efforts with multiple partners to combat the epidemic proactively and in its entirety.

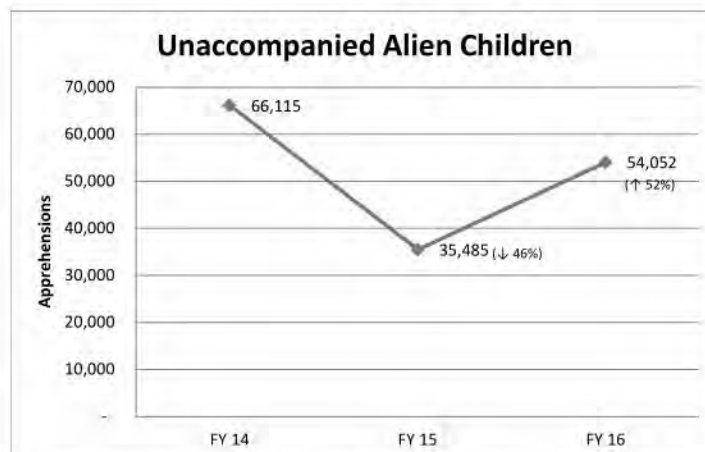
### *Human Smuggling*

- Families and unaccompanied children represent the most vulnerable of populations, and particular attention should be given to combat their human smuggling and the inherent abuse associated with it.
- Beginning in 2013, there was a massive surge of family and unaccompanied child apprehensions. The volume of families and unaccompanied child apprehensions at the Southwest Border have fluctuated over the last few years, with fiscal year (FY) 2016 apprehensions on pace to exceed those of prior years.

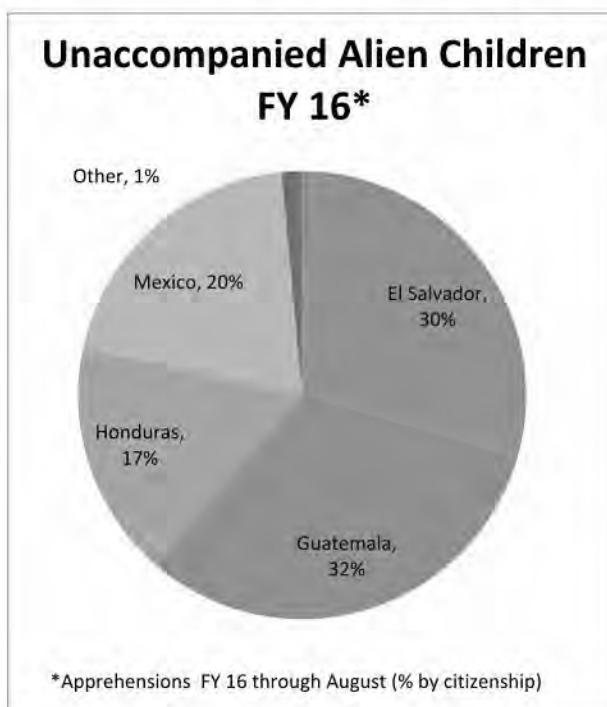
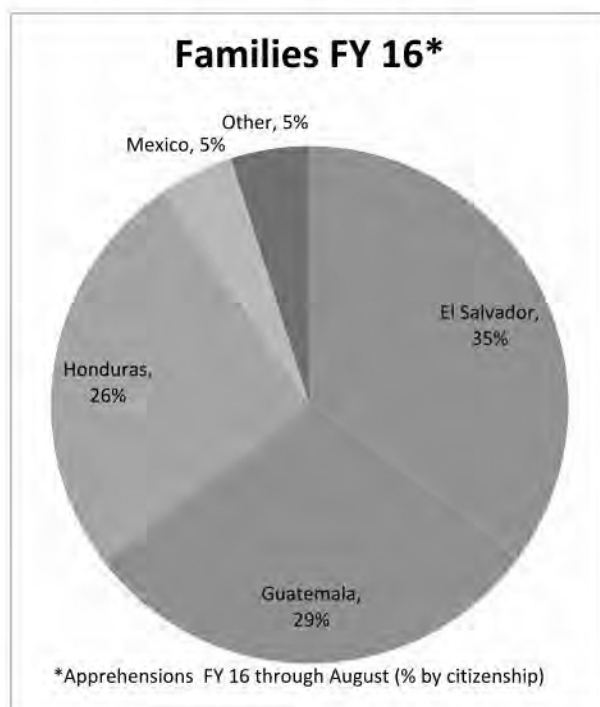


\*Represents the number of individuals (either a child under 18 years of age, parent or legal guardian) apprehended with a family member by the U.S. Border Patrol. Statistics as of 8/31/2016. Source: U.S. Border Patrol

- Apprehensions of families in FY 2016 have increased 97 percent over FY 2015 levels. Total family apprehensions this fiscal year are 68,080.
- Apprehensions of unaccompanied children in FY 2016 have increased 52 percent over FY 2015 levels. Total unaccompanied child apprehensions this fiscal year are 54,052.
- The U.S. Department of Health and Human Services, which takes custody of unaccompanied children, reports shifts in unaccompanied children demographics, particularly an increase in minors without family in the United States. Previously most unaccompanied children arrived with the intention to reunite with family members living here.
- The majority of unaccompanied children (98 percent) and families (95 percent) who are apprehended are nationals of El Salvador, Guatemala, Mexico, and Honduras.



\*Represents the number of individuals (either a child under 18 years of age, parent or legal guardian) apprehended with a family member by the U.S. Border Patrol. Statistics as of 8/31/2016. Source: U.S. Border Patrol



Statistics as of 8/31/2016. Source: U.S. Border Patrol



### *Challenges and Risks*

- Challenges to the dismantlement and disruption of human smuggling networks due to their decentralized nature and the relative ease of entry into the human smuggling services market by new facilitators. Even when whole networks are dismantled, the benefit is often temporary as new actors move to fill the vacuum in this very lucrative, low-risk enterprise.
- Due to its high potency and methods of exposure, the dangers associated with encountering, processing, and handling of evidentiary fentanyl-related compounds pose serious risks to field agents and other enforcement personnel. As such, current operational and procedural policies will likely need to be updated as well as the dedication of resources towards personal protective equipment for law enforcement personnel.
- Significant overdose encounters and deaths as well as existing threats that continue to evolve through the manufacture of fentanyl-related compounds.

[Return to Top](#)

## **COUNTERING VIOLENT EXTREMISM**

- The term “countering violent extremism” (CVE) refers to proactive efforts to prevent individuals from radicalizing to violence. This includes direct actions that counter extremists who attempt to radicalize, recruit, and mobilize individuals to violence, as well as forming community partnerships that mitigate conditions that relate to violent extremist recruitment and radicalization to violence. CVE efforts do not include gathering intelligence or performing investigations for the purpose of criminal prosecution or information sharing.
- Violent extremism is an evolving threat that increasingly involves terrorist-inspired attacks, as opposed to terrorist-directed attacks. These remote and decentralized activities lack common indicators historically used by traditional law enforcement and intelligence agencies, making it increasingly difficult to identify plots or aspirations to commit violence in the United States. Accordingly, DHS is incorporating CVE efforts into appropriate existing programs related to public safety, resilience, inclusion, and violence prevention.

[Return to Top](#)

## VETTING AND SCREENING

- Every day, DHS vets millions of individuals traveling to, from, or within the United States; applying for citizenship and immigration benefits; or seeking credentials, benefits, or other special access to secure areas of transportation.
- DHS, in partnership with our law enforcement and Intelligence Community colleagues, leverages a range of information and processes to conduct vetting and screening that support the prevention of terrorism and other operational missions.
- DHS utilizes biometric and biographic information collection; in-person interviews; research and analysis; database vetting and bulk data sharing; and publicly-available information to make risk determinations and inform decisions.

### *Current Trends/Operational Drivers*

- **Shared/Enterprise Services:** DHS is increasingly sharing vetting services across components, where appropriate, and utilizing enterprise services. For example, the Transportation Security Administration (TSA) conducts the vetting for a chemical facilities access security program run by the National Protection and Programs Directorate. DHS also maintains and operates a biometric database (IDENT) that is used broadly by the interagency.
- **Pushing security beyond the borders:** To support DHS's efforts to identify and address international threats as early as possible, operational programs (such as CBP's Preclearance and Trusted Traveler Program) provide opportunities for vetting travelers abroad and prior to travel to the United States, allowing for more efficient allocation of resources and increased ability to focus on unknown or potential threats.<sup>2</sup>
- **Social Media:** DHS is working to expand its current uses of social media to enhance existing vetting processes. Criminals and terrorists, whether intentionally or not, have provided previously unavailable information via social media that identified their true intentions
  - Social media is currently used by DHS Components for different operational or investigative purposes across DHS. DHS established a Social Media Task Force in December 2015 to examine the current and potential uses of social media within DHS, and how DHS could best expand its use (for screening and vetting programs).
  - USCIS and Science and Technology (S&T) conducted a number of pilots to automate bulk screening (with manual review) of social media information across a number of high priority application populations, including Refugees and Visa Waiver Program travelers.

[Return to Top](#)

## NATIONAL PREPAREDNESS SYSTEM

---

<sup>2</sup>CBP's Preclearance, operating at 15 locations worldwide, allows for advance inspection of passengers before they board U.S.-bound flights, while its range of international Trusted Traveler programs, provides pre-vetted and approved, low-risk travelers expedited clearance upon their arrival in the United States.

~~Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.~~

- The National Preparedness System was established to strengthen the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation. The National Preparedness System is an integrated set of guidance, programs, and processes to enable the Nation to meet the National Preparedness Goal, which is: “A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.”
- Nationwide, this translates into more disciplined and deliberate planning, organizing, equipping, training, and exercising among first responders, emergency managers, public health officials, and health care providers through their own investments as well as FEMA grants, which have totaled more than \$47 billion since 2002.
- The scope and scale of the National Preparedness System is both large enough and detailed enough to prepare for and use during catastrophic incidents as well as those managed by a single local emergency services organization. Using an all-hazards and whole community approach, the System is adaptable to all threats that the Nation faces.
- Through the National Preparedness System, FEMA assists the whole community in establishing goals, objectives, and performance measures that enable communities to measure improvements in capabilities and statewide preparedness.
- Within the annual National Preparedness Report (NPR), FEMA identifies progress and challenges to address in building and sustaining the Nation’s preparedness.
  - National areas for improvement include Cybersecurity, Economic Recovery, Housing, Infrastructure Systems, Natural and Cultural Resources, and Supply Chain Integrity and Security.
  - Three of these – (1) Cybersecurity, (2) Housing, and (3) Infrastructure Systems – have been identified as areas for improvement in the NPR for five consecutive years.
  - Capabilities that need to be sustained include Planning; Public Health, Healthcare, and Emergency Medical Services; and, Risk and Disaster Resilience Assessment.
- Maintaining and strengthening the National Preparedness System and building the capabilities of non-federal partners to reduce reliance on the Federal government, requires focused action in areas that include:





- Continue the development and implementation of the National Qualification System in order to advance integrated mutual aid across the whole community.
- Develop the guidance, tools, and technical assistance necessary to aid communities in building, sustaining, and delivering capabilities.
- Advance an integrated National Training and Education System that ensures the personnel responsible for delivering capabilities are receiving the right training at the right time.

[Return to Top](#)

## EMERGING INFECTIOUS DISEASE THREATS

- History has shown that highly infectious diseases emerge or reemerge with some regular frequency and could greatly hamper DHS's ability to perform critical mission functions. The impacts of these incidents on the United States, even if initially identified overseas, are exacerbated by factors such as globalization, international trade, reduced international travel times/enhanced travel routes, increased density of human populations in urban centers, and human encroachment into animal habitats.
- In close coordination with the Department of Health and Human Services (HHS) and the Centers for Disease Control and Prevention (CDC), DHS strives to protect the American public from emerging infectious disease (EID) threats through multiple actions such as:
  - Early warning from the National Biosurveillance Integration Center (NBIC);
  - Helping to prevent these diseases from crossing our borders; and
  - Coordination of the inter-agency response providing support to state, local, tribal, and territorial (SLTT) governments.
- DHS is also focused on protecting our workforce from EID threats, and ensuring the Department can continue to perform its critical missions in the face of these threats.
- The following trends are impacting the EID issue area, and will require changes in operational posture, policy, and/or resource allocation:
  - The threat has evolved. Over the past few years, we have seen numerous infectious diseases emerge with potential impacts to the American public and the DHS workforce, including H1N1, Ebola, and Zika. These outbreaks have required unprecedented levels of cooperation across DHS components and with interagency stakeholders.
  - Technological advancements have enhanced the ability to identify EIDs of potential concern (when in the past, they may have had been attributed to other etiologies).
  - The complexities of inter-agency response have increased with new capabilities in and responsibilities of some Departments and Agencies.
  - Since its launch in 2014, the Global Health Security Agenda (GHSA) has focused U.S. and international attention on building countries' capacity to help create a world safe and secure from infectious disease threats. Inherent to GHSA are requirements for participating countries to elevate global health security as a national priority in an effort to contribute to global health.
  - Government Accountability Office (GAO) reviews have found that DHS programs for biological early warning must evolve to meet today's threats. Success will require increased cooperation from external stakeholders (including federal partners).

[Return to Top](#)

## CHEMICAL THREATS

- (U//FOUO) DHS assesses that ISIL is increasingly interested in conducting and inspiring more complex attacks against the West<sup>3</sup>. ISIL-linked adversaries may consider incorporating toxic materials into attacks in the West with the aspiration of increasing fear, enhancing attack lethality, and adding greater complexity to response efforts. DHS believes that ISIL-inspired homegrown violent extremist (HVEs), or other domestic actors, who choose to pursue attacks with toxic materials most likely would employ commercially available toxic industrial chemicals (TICs) and use crude dissemination methods such as explosive dispersal, contaminating surfaces, poisoning food or water, or releasing gasses from pressurized tanks or via improvised chemical devices.
- When responding to a chemical attack, time matters for saving lives and managing resources. The window of opportunity to positively impact the response occurs in the first 2-4 hours. Most Federal resources are not available to support the immediate state and local response during that time. Therefore, the greatest Federal government impact to save lives must be made long before the incident occurs.
- Courses of action:
  - Work with chemical industry and the private sector to secure toxic chemicals in the supply chain.
  - Expand programs to train state and local first responders and leadership.
  - Maintain border and transportation security to stop bad actors before they have a chance to deploy chemicals as weapons.
  - Provide threat information and guidance to the state and local response community to enable a timely response and efficient decision making in the event of a chemical release.

[Return to Top](#)

---

<sup>3</sup> (U//FOUO) For more information please see DHS-FBI-Delaware Information Analysis Center-Ohio Strategic Analysis & Information Center Joint Intelligence Assessment "(U//FOUO) Toxic Materials Unlikely but Possible Weapon Choice for ISIL- Inspired or Directed Homeland Attacks" dated 23 May 2016

## **BIOLOGICAL THREATS**

- The nation faces risks from biological attacks or accidental releases of pathogens with the potential to produce destabilizing effects and greatly impact Department of Homeland Security (DHS) operations and the American public.
- The United States and its allies face ongoing and ever evolving threats from violent extremist groups or individuals inspired by these groups. The global reach of groups like Islamic State (IS) and the widespread availability of biological materials and expertise increase the risk of a terrorist attack using a biological Weapon of Mass Destruction (WMD).
- DHS's goal is to prepare our communities and our workforce to prevent, detect, mitigate, respond to, and recover from biological incidents quickly in order to save lives and minimize wide-spread or cascading impacts.
- The following trends are impacting the biological threats issue area, and will require changes in operational posture, policy, and/or resource allocation:
  - The threat continues to evolve. The biological weapons threat has expanded from large State-sponsored programs to include global terrorist groups and lone wolf violent extremists.
  - Government Accountability Office (GAO) reviews have found that programs for biological early warning must evolve to meet today's threats and provide the advanced warning needed to save lives. To achieve these ends the Department must foster increased cooperation across multiple partners and stakeholders, both within and outside the Department—to include various Federal partners.

[Return to Top](#)



## ENHANCING INTERNATIONAL AVIATION SECURITY

- Numerous attempted attacks and evolving, complex threat streams over the past decade clearly demonstrate terrorists' pervasive focus on targeting the aviation sector.
- A key mechanism for countering these threats is an informed, comprehensive application of security measures tailored to the threat and applied at those airports and air carriers most likely to be directly or indirectly affected.
- International inbound aviation represents the largest share of total aviation security risk (89%) for which the Transportation Security Administration (TSA) is primarily responsible.
- As such, TSA works closely with our U.S. Department of Homeland Security (DHS) partners, as well as foreign governments and industry stakeholders, to mitigate the risk on inbound international flights entering the United States. TSA also works closely with foreign governments to negotiate agreements to allow the carriage of Federal Air Marshals to and from Last Point of Departure airports.
- Since 2014, the total terrorist plots/attacks directed toward the West and Europe have increased over 73%.
- Recent aviation security incidents such as the terrorist attacks in Paris (November 2015) and Brussels (March 2016), the crashes of Metrojet 9268 in the Sinai Peninsula (October 2015) and Daallo Flight 159 in Somalia (February 2016), and the attack on the Istanbul Airport (June 2016) illustrate the need for consistent leadership engagement on international aviation security.
- The 114<sup>th</sup> Congress has provided a considerable amount of oversight on aviation security, passing legislation granting TSA new authorities for international engagement and requesting reports and oversight of international activities via the Federal Aviation Administration (FAA) Extension, Safety, and Security Act of 2016 (P.L. 114-190), which became law in July 2016.
- Per congressional request, the Government Accountability Office began in August 2016 an audit of TSA's foreign airport assessments and air carrier inspections; the completion date is to be determined.

[Return to Top](#)

## COMBATING TRANSNATIONAL CRIMINAL ORGANIZATIONS

- In 2011, the *National Strategy to Combat Transnational Organized Crime* was signed and stated in part “Criminal networks are not only expanding their operations, but they are also diversifying their activities, resulting in a convergence of transnational threats that has evolved to become more complex, volatile, and destabilizing. These networks also threaten U.S. interests by forging alliances with corrupt elements of national governments and using the power and influence of those elements to further their criminal activities.”
- Transnational criminal organizations (TCO) rely on revenues generated through the sale of illegal drugs, counterfeit goods, human trafficking and smuggling, and other criminal activities. These organizations, whether structured or decentralized in nature, continue to capitalize on technological innovation, including new platforms to sell illicit goods, innovative ways of moving money, tools for coordinating operations, and a variety of other criminal and cyber activities.
- Disrupting these complex illicit networks requires that DHS contribute to a well-informed and agile U.S. government and global response. Through integration of capabilities, DHS provides actionable, tactical and strategic intelligence and information across its operational component organizations. This not only enables unique DHS interdiction and investigative capabilities, but also those of domestic and foreign partners.

[Return to Top](#)

## REAL ID

- REAL ID<sup>4</sup> is a coordinated effort by the states<sup>5</sup> and the Federal Government to improve the reliability and accuracy of state-issued driver's licenses and identification cards (ID) in order to prevent the fraudulent issuance or use of these documents and, thereby, inhibit terrorists' ability to evade detection.
  - The REAL ID Act of 2005 ("the Act") (P.L. 109-13): 1) sets minimum requirements for the secure issuance and production of state-issued driver's licenses and IDs; and 2) prohibits Federal agencies from accepting driver's licenses and IDs issued by noncompliant states for official purposes (i.e., entering nuclear power plants, accessing Federal facilities including military installations, and boarding federally-regulated commercial aircraft).
  - It does not authorize DHS to: regulate states (state participation is voluntary); create a national ID; or create a Federal database of driver information.
- DHS has expended considerable effort to advance implementation of REAL ID through coordination with Governors, and their representatives, Department of Motor Vehicle Administrators, state legislators and national state associations.
- There are some states that have taken a "wait and see" stance to see if DHS is truly serious about REAL ID implementation and as a result, DHS has established strict enforcement dates.
- In 2017, DHS will: 1) determine whether states are compliant; 2) grant extensions to individual noncompliant states as appropriate;<sup>6</sup> and 3) prepare the public for enforcement related to boarding commercial aircraft.<sup>7</sup>
- The statutory requirements of the Act are the main driver for DHS enforcement.<sup>8</sup>
  - 13 states and 1 territory are not yet committed to becoming compliant (see Table 1 and Fig. 1) and could be affected when the Transportation Security Administration (TSA) begins enforcement on January 22, 2018. At that time, TSA will no longer accept licenses issued by noncompliant states (without extensions) for boarding commercial aircraft or entering an airport's sterile area.
- Potential courses of action include: adhering to the current enforcement plan; seeking statutory and regulatory changes to reduce compliance costs for states; or adjusting the enforcement schedule, which may necessitate regulatory changes.

---

<sup>4</sup> Not an acronym.

<sup>5</sup> "State" is defined as the 50 states; the District of Columbia; and the territories of American Samoa, Commonwealth of Northern Mariana Islands, Guam, Puerto Rico, and the U.S. Virgin Islands.

<sup>6</sup> Section 205(b) of the Act authorizes the Secretary of Homeland Security to grant states with an extension of time to meet the REAL ID requirements if the state provides adequate justification for noncompliance. Federal agencies may continue to accept driver's licenses and IDs issued by noncompliant states with an active extension.

<sup>7</sup> *Statement by Secretary Jeh C. Johnson on The Final Phase of REAL ID Act Implementation*. January 8, 2016. <https://www.dhs.gov/news/2016/01/08/statement-secretary-jeh-c-johnson-final-phase-real-id-act-implementation#>

<sup>8</sup> Under a 2012 interagency plan, the Federal Government has been phasing in REAL ID, an approach that has encouraged states to make progress by providing clear, realistic consequences for continued noncompliance.

[Return to Top](#)

## DHS BIG DATA

The Department of Homeland Security (DHS) is working to make its data a strategic asset for the homeland security enterprise to better inform operations, business processes, and decision-making.

The DHS Data Strategy will provide a foundation of enterprise data management values, guidelines, and principles to leverage its data assets to create value in five (5) major areas:

Mission	Risk-based priorities requiring enterprise-wide data management including, but not limited to: screening and vetting, threat assessment, and distribution of assets for response and protection. Early successes have been achieved in this area through leading projects like the DHS Data Framework for the Homeland Security Intelligence Enterprise, DHS Office of Policy's Immigration Data Integration Initiative, and Science & Technology Directorate's (S&T) Homeland Security Advanced Research Projects Agency's (HSARPA) Data Analytics Engine (DA-E).
Management	Enterprise priorities for understanding, organizing, analyzing and making management decisions. Early success in this area has already been seen with the Management Directorate's Management Cube, an innovative solution that brings together essential management data to enhance decisions and performance.
Planning	Supporting and driving DHS strategic planning by using enterprise data management to support risk assessment, resource allocation, and performance assessment.
Research	Rapid evaluation of emerging big data and advanced computational techniques that are relevant to significantly improving the leveraging of DHS data, and prioritized delivery of enterprise services. HSARPA's Data Analytics Engine works across industry, academia and government to understand rapid technical innovations that create opportunities and risks for homeland security mission.
Enterprise Service Delivery	The DHS Office of the Chief Information Officer (OCIO), with Component partners, plays a lead role in delivering enterprise services for data management.

### Course of action:

Leadership and Priorities	Enterprise data management shall be governed under the Information Sharing and Safeguarding Governance Board (ISSGB) and establish a network of component-level Chief Data Officers (CDOs), to be coordinated under the oversight of the ISSGB.
Standards and Enforcement	DHS shall define and enforce standards for enterprise data management.
Compliance	The Department must ensure that it complies with all legal and policy requirements in the maintenance collection, use, and dissemination of its data.
R&D	S&T leads the Department's efforts to innovate and evaluate emerging big



	data solutions and related technologies to provide technical guidance, consultation and potential solutions for missions of Homeland Security Enterprise.
Enterprise Technology Development	DHS carefully develops, leverages and deploys efficient technologies to meet current data management needs. The DHS OCIO, with Component partners, will play a key role in delivering enterprise services for data management.
Communications	DHS effectively communicates, and understands, the value of data management, from not only leadership, but from operators, analysts and planners who know what they need from our DHS data.

[Return to Top](#)

## **PREVENTING NUCLEAR TERRORISM**

- The grave threat of nuclear terrorism against our nation has been stressed by the current U.S. president and his predecessor. A terrorist nuclear attack could involve one or more nuclear devices, each with an explosive yield sufficient to cause massive casualties and devastation to a metropolitan area, damaging the nation's sense of security and resulting in major worldwide disruptions to commerce, trade, and travel.<sup>9</sup>
- Because of the catastrophic consequences, the Department must continue to prioritize prevention of nuclear terrorism. Bolstering capabilities at the federal, state, local, territorial, and tribal levels helps defend the nation. Working with the international community helps to enhance nuclear security worldwide, well beyond our borders.
- But maintaining an appropriate sense of urgency towards low-probability, high-consequence threats such as nuclear terrorism is challenging. Other, more likely threats may demand more immediate attention. Ensuring that the homeland security enterprise is engaged in preventing a potentially catastrophic terrorist nuclear attack is critical.

[Return to Top](#)

---

<sup>9</sup> Alternatively, a "dirty bomb," dispersing radioactive material using conventional explosives, could deny access to a portion of a city for some time but cause significantly fewer deaths.

## ARCTIC / POLAR

- Access to Arctic sea routes is increasing due to climate change and improved vessel capabilities (e.g. Polar Code compliant vessels).
- Diminishing Arctic sea ice may provide shippers a substantially shorter route between Asia and Europe, and opens larger areas to natural resource exploration/exploitation not only at sea but also within United States Arctic terrestrial domain (e.g., rare earth metals in northern Alaska).
- Increased global access to the Arctic may present challenges to U.S. sovereignty, especially in areas where there are competing claims to the Outer Continental Shelf, exacerbated by the U.S. not being a signatory to the United Nations Convention on the Law of the Sea.
- Conflicting territorial claims in the Arctic may present challenge to U.S. position on freedom of the seas and navigation, including disputes with Canada.

### *Importance*

- The U.S. is an Arctic nation and must maintain the ability to protect U.S. borders, exert our sovereignty over our territorial seas and Exclusive Economic Zone, and ensure the safe, secure and environmentally-responsible maritime activity in U.S. Arctic waters.

### *Trends*

- Trend 1: The Arctic is warming at a faster pace than the rest of the world – nearly twice the global rate over the last 100 years – which has led to diminishing sea ice and increased access to Arctic sea routes. The pace of warming has accelerated markedly in the past three decades.
- Trend 2: Increased maritime activity, including commercial shipping (passenger and cargo), energy exploration and exploitation, and recreational vessels will use Arctic sea routes in or adjacent to U.S. waters.
- Trend 3: Increasing maritime activity funnels through “choke points” such as the Bering Sea, significantly elevating risks within traditional Coast Guard missions (e.g., Search and Rescue, or SAR).
- Trend 4: Arctic and non-Arctic nations and states have increased their focus on producing polar-capable vessels and icebreakers to enable shipping through Arctic sea routes, providing both partners and competitors with greater Arctic access than that of the U.S.

### *Major Risks*

- Increased human activity in the Arctic presents risks to the integrity of U.S. borders and environmental and maritime safety risks associated with trans-Arctic shipping and mineral exploration/exploitation.
- The remote and harsh nature of the Arctic and lack of infrastructure (including ports, navigational aids, reliable hydrographic data, and communications) and the lack of consistent adequate domain awareness creates a difficult incident management posture.

### *Courses of Action*

- Course of Action 1: Maintain year-round Polar access via icebreakers and air capabilities.
- Course of Action 2: Build robust partnerships with states and groups with Arctic equities and expertise.
- Course of Action 3: Work cooperatively to protect the Arctic's rich marine environment.



Arctic Boundary as defined by the Arctic Research and Policy Act (ARPA) of 1984, Public Law 98-373, at 15 USC §4111.



The Coast Guard Cutter Polar Star, the nation's only heavy polar icebreaker, cruises on the ice edge of the Chukchi Sea north of Wainwright, Alaska, in July 2013. (PETTY OFFICER 1st CLASS Sara Mooers / U.S. Coast Guard)  
Source Publication: <http://www.adn.com/opinions/2016/08/15/u-s-needs-more-icebreakers-to-keep-watch-in-arctic/>

[Return to Top](#)



## **INFORMATION SHARING WITH FOREIGN PARTNERS**

- The DHS Office of Policy (PLCY) coordinates all DHS engagement with foreign governments and international organizations. PLCY works closely with the DHS Components, as the operators that implement any international information sharing arrangements, to ensure agreements and arrangements are in support of and alignment with Departmental international engagement priorities.
- DHS works closely with the Departments of State and Justice, where applicable, when negotiating new arrangements that may impact the U.S. government.
- DHS regularly shares information with U.S. government intra-agency partners and key foreign partners to aid in the identification of criminals, terrorists and illegal immigrants before they can target the United States or our allies for nefarious purposes.
- Data shared may be derogatory in nature (e.g. criminal histories, immigration violations, or terrorist watchlists), transactional (e.g. travel history) or identity (e.g., names).
- International information sharing activities are influenced by legal, operational and policy frameworks, and the nimble threat environment. Such factors may include, but are not limited to:
  - The Visa Waiver Program (VWP) requirements;
  - Global migration trends, including from Central America to the U.S. and from the Middle East to Europe;
  - Exploitation of global travel systems by foreign fighters;
  - Mandate to identify, dismantle, and/or disrupt Transnational Crime;
  - The potential for criminals and terrorists to circumvent some U.S. screening programs by obtaining new identities and travel documents in third countries;
  - U.S. legislation that prohibits the use of criminal history for immigration or non-law enforcement purposes;
  - International debates over privacy particularly within the European Union.

[Return to Top](#)

## REFUGEE PROCESSING AND VETTING

- Every year, immigration law requires that Executive Branch officials to consult with members of the Committees of the Judiciary in the Senate and House of Representatives regarding:
  - Review the refugee situation or emergency refugee situation.
  - Project the extent of possible participation of the United States in resettling refugees.
  - Discuss the reasons for believing that the proposed admission of refugees is justified by humanitarian concerns, grave humanitarian concerns or is otherwise in the national interest.
- Following the Consultations, the Department of State drafts a Presidential Determination for signature by the President, which establishes the overall admissions levels and regional allocations of all refugees for the upcoming fiscal year. The Department of State has the lead in arranging the Consultations. No refugees may be admitted in the new fiscal year until the Presidential Determination has been signed.
- On an annual basis, processing priorities are established that determine which of the world's refugees are "of special humanitarian concern to the United States," i.e., eligible to be considered for possible resettlement in the United States. The priorities currently in use are:
  - P-1: United Nations High Commissioner for Refugees, U.S. Embassy, or non-governmental organization (NGO) identified cases, including persons facing compelling security concerns, women-at-risk, victims of torture or violence and others in need of resettlement
  - P-2: groups of special concern identified by the U.S. refugee program (e.g., Bhutanese in Nepal)
  - P-3: family reunification cases (i.e., spouses, unmarried children under 21, and parents of persons lawfully admitted to the U.S. as refugees or asylees or persons who are legal permanent residents or U.S. citizens who previously had refugee or asylum status)
- Eligibility for refugee status is decided on an individual, case-by-case basis. A USCIS officer conducts an in-person interview of the applicant that is non-adversarial and designed to elicit information about the applicant's claim for refugee status. During a refugee interview, an officer confirms the basic biographical data of the applicant; verifies that the applicant was properly given access to the USRAP; determines whether the applicant has suffered past persecution or has a well-founded fear of future persecution, on the basis of political opinion, religion, nationality, race, or membership in a particular social group in their home country; determines whether the applicant is firmly resettled, is barred for persecution of others, and is admissible to the United States; and assesses the credibility of the applicant.
- All refugees are subject to the highest level of security checks of any category of traveler to the United States, including the involvement of the National Counterterrorism Center, the

FBI's Terrorist Screening Center, the Department of Homeland Security, the Department of State and the Department of Defense. All refugees, including Syrians, are admitted only after successful completion of this stringent security screening regime.

- Security checks are an integral part of the USRAP for applicants of all nationalities, and coordinating these checks is a shared responsibility between the Department of State and DHS.
- All available biographic and biometric information is vetted against a broad array of law enforcement, intelligence community, and other relevant databases to help confirm a refugee applicant's identity, check for any criminal or other derogatory information, and identify information that could inform lines of questioning during the interview.
- These checks are completed by the Department of State, DHS, the Federal Bureau of Investigation, and the intelligence community.
- A refugee applicant cannot be approved for travel until all required security checks have been completed and cleared.

[Return to Top](#)