Open Government Plan 3.0

U.S. Department of Homeland Security

Homeland Security

Letter from the Acting Under Secretary for Management

I am pleased to release the Department of Homeland Security's Open Government plan version 3.0. This plan builds upon the success of the prior plans and focuses on how the tenets of Open Government support the DHS Mission. The Administration set the vision for Open Government in 2009 with President Obama's Memo on Transparency in Government and the follow on Open Government Directive from the Office of Management and Budget. Throughout his Administration, the President has prioritized making government more open and accountable, and has taken substantial steps to increase citizen participation, collaboration, and transparency in government.

At the inaugural Open Government Partnership meeting on September 20, 2011, President Obama reiterated his belief "that the strongest foundation for human progress lies in open economies, open societies, and in open governments." The United States has worked both domestically and internationally to ensure global support for Open Government principles to promote transparency; fight corruption; energize civic engagement; and leverage new technologies in order to strengthen the foundations of freedom in our own nation and abroad."

In December 2013, the Obama Administration released the second "Open Government National Action Plan for the United States of America," which included 23 new or expanded open government commitments. The new National Action Plan gives us more guidance for improving the pillars of transparency, collaboration, and participation and is integrated into our new plan. The new plan expands upon our efforts to modernize the Freedom of Information Act processes, improve public participation, increase transparency in government spending, and open government data through various existing and new initiatives.

In an on-going effort to support the National Action Plan and the Open Government Directive, and in consideration of stakeholders from the private and public sectors, I am proud to release the DHS Open Government plan version 3.0. Building upon plan versions 1.0 and 2.0, plan version 3.0 continues the great work that was started and identifies new flagship initiatives to further promote Open Government. In addition, this plan highlights:

- The Department's compliance with the Open Data Memorandum M-13-13;
- The Department's plans to proactively disclose information to advance transparency, accountability, and the presumption of openness;
- Privacy compliance reports;
- Whistleblower Protection; and
- Digital Strategy Website.

– Under Secretary, Management (acting), Chris Cummiskey

Table of Contents

I. Background and Governance

After the Office of Management and Budget released the Open Government Memorandum in 2009, the Secretary of Homeland Security designated the Management Directorate to lead the implementation of Open Government. In fiscal year 2010, the Deputy Under Secretary for Management signed Open Government plan version 1.0 which explored current activities that exhibit open government in DHS and charted a path forward for increasing participation, collaboration, and transparency in support of the Open Government initiative.

In fiscal year 2011, DHS renewed its commitment to Open Government as it released plan version 2.0 which outlined new Open Government efforts including:

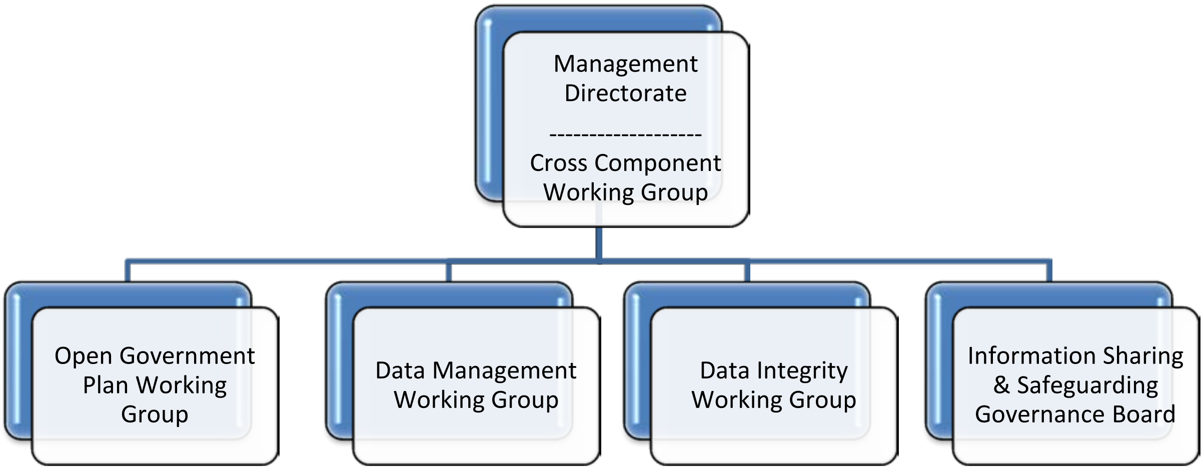
- Hosting open dialogues to receive comments and ideas from the public on cybersecurity and National Preparedness using General Services Administration's online collaboration tool IdeaScale;
- Updating the Department's social media tools; and
- Providing additional datasets to data.gov, the main portal for providing the public access to the high value, machine-readable datasets generated by the Executive Branch.

In fiscal year 2012, DHS released an addendum to plan version 2.0 which highlighted the Department's transparency initiatives and efforts around improving customer service, including:

- The Department's ongoing and new efforts to improve proactive disclosure and reduce Freedom of Information Act (FOIA) backlogs;
- Targeted datasets that provide valuable safety information to the new platform, Safety.data.gov;
- Geospatial data, information and images;
- A focus on customer service through web interface and public outreach; and
- Existing and new Flagship Initiatives.

Open Government Governance

At the direction of the Deputy Under Secretary, the Management Directorate convened a cross-component working group to address the Open Government Directive deliverables, evaluate how to best incorporate the directive into the Department's processes, and establish performance measures to gauge the Department's progress in incorporating the Open Government Plan into its operations. In addition, the Department convened several working groups in support of Open Government as outlined in the next section.


Management Directorate

Cross Component Working Group
Open Government Plan Working Group
Data Management Working Group
Data Integrity Working Group
Information Sharing & Safeguarding Governance Board

Figure 1. Open Government Governance

Working Groups

Open Government Plan Working Group

The Management Directorate convened a cross-component working group to address the deliverables required in the Open Government Directive and ensure that the Open Government Plan reflects the operations of the Department. This group meets monthly or on an as-needed basis to discuss progress, roadblocks and new ideas for the Department's continued evolution of the three pillars of Open Government. In addition, the working group receives updates from the Data Management Working Group, the Data Integrity Working Group and other DHS Components who are part of the Open Government community.

Data Management Working Group

Established by the Enterprise Data Management Office, the Data Management Working Group defines, promotes and monitors Enterprise Data Management practices. Such practices achieve the objectives of information sharing, discovery, and reuse for and within DHS. This working group enables DHS Components and partners to:

- Harmonize their enterprise data management decisions;
- Promote the conditions for information sharing across DHS;
- Identify data security, privacy and classification initiatives; and
- Lay the foundations for extensible interoperability across the broader Homeland Security community

The working group is the official vetting mechanism for all issues related to the Data Reference Model portion of the Enterprise Architecture, including insertions into the architecture for data assets, standards, and information exchanges. The members of the working group make recommendations that are then carried forward to the Enterprise Architecture Center of Excellence, which votes on recommendations to be brought before the Enterprise Architecture Board for final approval.

Data Integrity Working Group

The DHS Chief Financial Officer has been designated the Senior Accountable Official for Data Quality under this directive and is working across DHS on data quality improvements, including working closely with senior leaders engaged in procurement/acquisition actions and those engaged in financial assistance program administration. The CFO provides guidance and oversight for components to perform periodic reconciliation of their financial reporting data submitted to OMB against the publically available spending data posted on USASpending.gov, and also for components' performance of sample testing at transaction level (e.g., individual contracts and grants). The Under Secretary for Management has requested each component designate an Accountable Official to work with the CFO to ensure internal controls to support the integrity of financial data being released to stakeholders via the Department's website, USASpending.gov, Data.gov and other electronic and print mediums. The Senior Management Council provides ongoing reviews, advice and ongoing oversight to this critical set of activities, much as it has throughout the various internal control activities required by OMB Circular A-123: Management's Responsibility for Internal Controls. DHS is leveraging existent, effective infrastructure to accomplish key objectives.

Information Sharing and Safeguarding Governance Board

The Information Sharing and Safeguarding Governance Board (ISSGB) is comprised of executive leaders from the components to ensure the flow of information across the Department. Mandated by the 2007 "One DHS" Memo as the decision-making and steering committee of the DHS Information Sharing Governance Structure, the ISSGB arbitrates inter-component information access delays and denials, leads the development and implementation of strategy guiding DHS information-sharing and collaboration activities, and ensures that the Department speaks with "one voice" to its external partners.

Offices

In addition to the working groups used to oversee Open Government, the offices identified below represent the pillars of Open Government in their day to day operations. Each entity provides significant ongoing support and oversight in the implementation of the Open Government Plan at DHS.

Privacy Office

The Department of Homeland Security Privacy Office is the first statutorily-required privacy office of any federal agency. The Privacy Office is responsible for managing Freedom of Information Act, Proactive Disclosures, and Privacy matters for the Department.

Functions of the Privacy Office include:

- Evaluates Department legislative and regulatory proposals involving collection, use, and disclosure of Personally Identifiable Information (PII);
- Centralizes FOIA and Privacy Act operations to provide policy and programmatic oversight, and support implementation across the Department;
- Operates a Department-wide Privacy Incident Response Program to ensure that incidents involving PII are properly reported, investigated and mitigated, as appropriate;
- Responds to complaints of privacy violations and provides redress, as appropriate; and
- Provides training, education and outreach to build a culture of privacy across the Department and transparency to the public.

Office of the Chief Financial Officer

The Chief Financial Officer serves as the Senior Accountable Official for the DHS Data Quality Plan for Federal Spending Information in support of the Open Government Directive. Recently the CFO formed the Council Chief Executives of Financial Assistance and underneath this body, the Council Heads of Financial Assistance Activities. Both of these workgroups assist the CFO with his efforts of providing quality federal financial assistance spending information. The CFO provides oversight and guidance to ensure internal controls support the integrity of grant, loan and contract information posted publicly on USASpending.gov and that adequate internal controls are in place for that information.

Office of Public Affairs

The Office of Public Affairs (OPA) coordinates the public affairs activities for the entire Department, serving as the federal government's lead public information office during a national emergency or disaster. OPA includes the Press Office, Incident and Strategic Communications, Speechwriting, Public Web Management, and Internal Communications. All of these offices work in tandem to support comprehensive information flow about the Department and its missions to the public, media and employees. The Office of Public Affairs coordinates the maintenance of the Department's official public website: www.DHS.gov.

Office of Intergovernmental Affairs

The Office of Intergovernmental Affairs (IGA) promotes an integrated national approach to homeland security by coordinating and advancing federal interaction with state, local, tribal, and territorial governments. IGA is responsible for opening the homeland security dialogue with executive-level partners at the state, local, tribal, and territorial levels, along with the national associations that represent them.

Office for Civil Rights and Civil Liberties

The Office for Civil Rights and Civil Liberties (CRCL) supports the Department's mission to secure the nation while preserving individual liberty, fairness, and equality under the law. One way in which CRCL integrates civil rights and civil liberties into DHS activities is by fostering ongoing communications and building lasting relationships between the Department and the public. CRCL engages with the public through a number of collaborative engagement efforts with communities to improve channels of communication and inform the Department about the concerns of affected communities.

Private Sector Office

The Private Sector Office (PSO) is the primary advisor to the Secretary of Homeland Security on issues related to the private sector, including business, academia, non-profits, and nongovernmental entities. PSO coordinates active engagement between DHS and the private sector to build strong partnerships, shape policy, and enhance internal and external dialogue.

Office of Legislative Affairs

The Department values communications with Congress. The Office of Legislative Affairs (OLA) serves as primary liaison to Members of Congress and their staffs. The office responds to inquiries from Congress; notifies Congress about Department initiatives, policies, and programs; and keeps Congress informed by providing timely information about Homeland Security and national security matters. OLA accomplishes this through briefings, testimony, background information, staff discussions and field visits for Members of Congress or their staffs to gain a better understanding of DHS operations. OLA communicates accurate and detailed information to congressional interests, while following appropriate protocols to safeguard classified or otherwise sensitive information.

II. New Flagship Open Government Initiatives

The Department of Homeland Security has two new flagships that support the core objectives of the Open Government Directive; the U.S. Customs and Border Protection (CBP), Automated Commercial Environment and the Federal Emergency Management Agency, OpenFEMA program. The Department is also reporting updates to the flagships identified in the previous Open Government Plan for the National Information Exchange Model and the Office of Academic Engagement.

Flagship 1: U.S. Customs and Border Protection: Automated Commercial Environment "Single-Window"

Overview:

Forty-seven federal agencies are involved in the largely manual and paper-based trade process, which is costly and time-consuming for both the Government and the international trade community. Approximately 30 agencies require nearly 200 forms for the importation and exportation of cargo. The Security and Accountability for Every Port Act of 2006 (SAFE Port Act) directed all agencies that require documentation for the import and export of cargo to participate in International Trade Data System (ITDS) to establish a single portal system for the collection and distribution of trade data. Through the ITDS initiative, the federal government is creating a Single Window to transform and streamline the trade process, thereby supporting economic competitiveness. The U.S. Single Window will set the stage for international harmonization with other like-minded countries pursuing trade simplification.

On February 19, 2014, the President signed an Executive Order (EO) on *Streamlining the Export/Import Process for America's Businesses*. The EO establishes a phased approach to meet the December 31, 2016 deadline for completion and government-wide use of the ITDS Single Window, prioritizing inclusion of agencies playing a major role in cargo movement.

The U.S. Customs and Border Protection Automated Commercial Environment (ACE) will become this Single Window– the primary system through which the international trade community will submit import and export documentation required by all federal agencies. ACE is the technology that will enable Single Window trade processing. Through ACE, federal agencies will have earlier, automated visibility to shipment data, expediting their import or export assessments at the border and speeding the flow of legitimate trade while also improving security, health and safety of cargo.

ACE development has been underway for more than 10 years and significant capabilities have been developed and deployed; these capabilities have streamlined business processes and resulted in significant savings for CBP and industry. CBP is on track to develop and deliver remaining core trade processing capabilities in ACE and decommission the corresponding capabilities in legacy systems by the end of calendar year 2016.

Public Engagement:

CBP is working very closely with the private sector on the development of ACE/ITDS capabilities. CBP employs an iterative, flexible consultative process focused on building partnership and trust, providing transparency and producing results that are mutually beneficial to government and industry. Two key private sector groups serve as the voice of the international trade community and provide direct input to CBP on the development of ACE/ITDS:

- **Commercial Operations Advisory Committee (COAC) of CBP –** The COAC provides recommendations to CBP from an industry perspective. Three sub-committees within the COAC provide strategic recommendations and input on Border, Exports, and Modernization.

- **The Trade Support Network (TSN)** is a group of more than 300 members from across all sectors of the international trade community. The TSN works through nine sub-committees to provide tactical input on ACE/ITDS development and capabilities. The TSN helps define requirements from an industry perspective, identify enhancements to existing functionality and assist CBP with testing capabilities prior to deployment.

In addition to these public forums, CBP has a support network similar to the TSN that ensures the voices of CBP field personnel are heard and their needs are represented during development.

The EO establishes a two-tiered governance structure to allow those with technical expertise to engage on the development of the Single Window while policy makers focus on improving border management policies and processes across the U.S. Government and in partnership with non-governmental stakeholders.

The existing ITDS Board of Directors, established under the SAFE Port Act of 2006, and chaired by the Secretary of the Treasury, will continue to oversee the development of the Single Window through ACE/ITDS. The ITDS Board of Directors includes representatives from all 471 ITDS partner government agencies-to ensure interagency collaboration.

The newly expanded Border Interagency Executive Council (BIEC) is responsible for improving coordination among the 47 agencies, such as the Department of Transportation, Department of Commerce, and Consumer Product Safety Commission, with border authorities and between the U.S. Government and other stakeholders. The goal of the BIEC is to cut red tape and reduce supply chain barriers to trade.

Measuring Progress:

A key component of the Single Window initiative is the elimination of cumbersome paper-based processes and the automation of forms required by the Government for the importation and exportation of goods. Two key measures will be used to measure inter-government progress on the initiative: (1) the number of forms automated; and (2) number of forms eliminated.

Sustainability and Continuous Improvement:

CBP is using an Agile development methodology to build ACE/ITDS, along with open standards and code that can be reused across processes. The system is being built as a series of services, using a service oriented architecture, so that functionality can more easily, and cost effectively, be modified as needed as time progress. Agile is an intensely user-centric methodology where stakeholders work side-by-side with developers to ensure capabilities reflect the needs of all users. While core functionality will be completed and the Single Window will be implemented by the end of 2016, work to continually streamline trade processes and enhance technology for the ever changing trade environment will not stop.

FLAGSHIP 2: FEDERAL EMERGENCY MANAGEMENT AGENCY – OPENFEMA

Overview:

OpenFEMA is the Federal Emergency Management Agency's open government initiative and modernization project. Developed with specific Congressional appropriations, the program embraces the tenets of transparency, participation, and collaboration. It supports citizens and first responders while increasing government accountability, innovation, and effectiveness. Led by FEMA's Chief Technology Officer, OpenFEMA launched in October 2012 within the FEMA Office of the Chief Information Officer (OCIO) with the mission to expand and promote a culture of open government among FEMA and the whole community in support of the nation's ability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

In its first year (2012-2013) OpenFEMA identified the following program goals:

- Release data for public consumption, and
- Engage with external stakeholders to leverage FEMA's data.

For 2013-2014 OpenFEMA added the following goal:

- Institutionalize the data release processes and opportunities for the whole community to effectively use the data.

Building off the Department's Open Government plan, OpenFEMA takes steps to proactively publish data sets in open formats that are easily accessed by citizens as well as private sector and non-governmental organizations. In OpenFEMA's first year, 2012-2013, the team created a process to facilitate and prioritize the release of data at FEMA and encourage innovation with internal and external stakeholders. This process was later adopted Department-wide. In its first year, OpenFEMA also accomplished the following:

- Launched the:
  - OpenFEMA web page www.fema.gov/open
  - Developer web page www.fema.gov/developer
  - OpenFEMA email openfema@fema.dhs.gov
- Began developing an application programming interface (API) to provide machine-to-machine public data access
- Released 24 datasets
- Sponsored the National Day of Civic Hacking

Transparency, Participation, and Collaboration:

To engage with internal stakeholders and release data, OpenFEMA partnered across the agency with the Office of External Affairs (OEA) to communicate the tenets of open data, including the importance of data transparency and collaboration. Working closely with program offices, the OpenFEMA team continues to learn what data is available to address the needs of stakeholders. Together with the program offices, OpenFEMA helps determine data priority and packages the datasets for public release. Through the OEA's Private Sector Division, OpenFEMA engaged with existing FEMA partners across commercial, not-for-profit, academic, and government sectors. The initiative also reaches external stakeholders through the OpenFEMA website, email, IdeaScale (a collaborative idea engine), and social media channels. OpenFEMA encourages users to submit data recommendations, feedback, and provide insights on how they are using FEMA's data. In its first year, OpenFEMA directly engaged with more than 60 private sector and government partners in an effort to expand data standards. These partnerships span the commercial, academic, and not-for-profit sectors, and over 23 offices and programs throughout the federal government, external to FEMA and DHS.

Moving forward in 2014 – People First, Ideas Second, and Hardware Third:

Scattered throughout the Agency and the whole community—including disaster survivors—are numerous individuals who are innately innovative and interested in designing and developing solutions to build resiliency and improve our nation's response to catastrophic events. These individuals should be empowered to create and accelerate an inventive and innovative culture throughout the whole community. OpenFEMA will continue to foster innovation through using the following approach:

- <u>People First</u>: Build ideas, concepts, and system solutions around people, not the other way around. Put simply, our approach to technology needs to place people first.
- <u>Ideas Second</u>: Standards support the ideas which empower people to achieve outcomes. All ideas reflected in standards—comprised of practices and policies inside and outside government across the whole community—must lead to the empowerment of people to achieve outcomes.
- <u>Hardware Third</u>: Processes support the systems and hardware that embody the standards and ideas which empower people to achieve outcomes. Only after supporting the standards, which enable people to achieve outcomes, should there be a consideration of solutions, systems, and overall processes within an organization.

OpenFEMA will continue to provide the whole community with access to historical and recent data. Providing greater access to FEMA data follows a broader, government-wide trend that results in independent data analysis and visualization. To do this, OpenFEMA will work towards institutionalizing programs and processes throughout FEMA, thus empowering program and regional offices to release data and engage with their external stakeholders to address needs unique to their communities.

Disaster Response & Recovery – Year One Accomplishments

Using FEMA's Open Data to More Effectively Rebuild after Hurricane Sandy:
Community organizations, non-profits, and state and local governments had a critical need for comprehensive data to understand the full impact of Hurricane Sandy. These stakeholders required data to properly determine the need for a range of housing programs to complete the newly required impact and unmet needs assessments required by HUD for the use of approximately $5.5 billion in Community Development Block Grant funds. OpenFEMA facilitated the release of an aggregated, non-PII dataset from the FEMA Individual Assistance Program for New York and New Jersey. This allowed stakeholders to make data-informed decisions regarding the design and allocation of federal funds for the recovery after Hurricane Sandy. FEMA created the dataset elements using knowledge from past experience and available information, such as post-disaster information request trends as well as stakeholder input.

Partnering for More Searchable and Discoverable Data during Disasters:
After major disasters like Hurricane Sandy, many survivors require disaster assistance in real time and search engines need accurate, reliable data about available FEMA resources, such as Disaster Recovery Centers (DRCs). OpenFEMA responded by providing search engines with FEMA DRC data that included the DRC locations, directions on how to get there, and contact information. Google Crisis maps and other search engines provided this information when disaster survivors searched for it from their computers or mobile devices. This data was also made available on www.fema.gov/data, which allowed anyone to utilize the data for their website, application, or other analysis tool. Google Crisis Map received 15 million queries for Sandy-related information, while FEMA had 740,000 visitors to its Sandy pages, and USA.gov had 71,000 visitors to the main government-wide Hurricane Sandy page.

Stewarding an Innovation Ecosystem: Soon after Hurricane Sandy made landfall, FEMA identified real-time challenges, including the need for a shared space to virtually connect and leverage resources to solve issues. Within 48 hours, OpenFEMA provided an agile workspace that helped to increase collaboration even with differing domains and access points, spur innovative ideas, and share resources that supported disaster survivors. Examples include, but are not limited to: providing internet connectivity at Red Hook, Rockaways, Staten Island and other affected communities, which allowed FEMA Corps volunteers to go door-to-door and register disaster survivors from their door-steps. This also had the effect of freeing up Mobile Communications Operations Vehicles (MCOVs), a limited resource, to go into other affected areas and meet survivor needs.

Streamlined SRIA Reporting and Access: FEMA has been implementing the Sandy Recovery Improvement Act of 2013 (SRIA), and OpenFEMA has supported this implementation. For example, as of August 1, 2013, OpenFEMA is managing the daily Public Assistance Awards and the Mission Assignments data and is working to have the reports automated as part of the upcoming API platform. Data is now publicly accessible in open formats, satisfying statutory requirements. Publishing in an open format has not only saved processing time, but also allows for end users to compile the data and sort through it more efficiently and in additional value-added ways.

Innovation for Urban Search and Rescue: Developers and local citizens wanted to help develop a resource that would support their local first responders after the Moore, Oklahoma category 5 tornado. In their efforts, they learned that no existing tools allowed for local and state Urban Search and Rescue teams to share data. OpenFEMA coordinated with local developers and private citizens at a nearby event, which led to the creation of an open source urban search and rescue mobile application that is free and allows for creation of a better common operating picture. These efforts increased the efficiency of response and recovery efforts and their application received the White House Champions of Change award.

Process Improvement – Year One Accomplishments

Providing High Volume Datasets via Application Programming Interfaces:
Prior to OpenFEMA, FEMA did not have a platform for machine-to-machine data feeds for public access. The OpenFEMA team developed the initial API platform that provides multiple datasets in open and accessible formats. This platform makes it easy to add additional datasets with minimal development effort. Currently the team is working with the Department's Chief Information Officer team to complete testing and implement redundancy for the API platform. As part of our initial implementation, a user is able to request a full or partial bulk download of any of our publicly available datasets in popular data exchange formats such as JavaScript Object Language (JSON), geographic features enabled JSON (GeoJSON), or comma separated values format.

Establishing a Clear Data Release Process that Ensures Privacy and Confidentiality:
The OpenFEMA team established the FEMA data release process. This process included the formation of a data review team, which includes Office of Chief Counsel, the FEMA Privacy Office, Public Affairs, External Affairs, and Operations Security, in addition to the relevant program office. OpenFEMA designed the release process based on open government policy standards and an internal understanding of FEMA's culture. This action has allowed for the Agency to release and update 24 datasets and has led to more transparency and collaboration with external stakeholders, efforts which help build stronger public trust and innovation for planning, response, and recovery efforts.

Collaborating with Internal and External Champions:
OpenFEMA implemented an integrated communications plan to increase knowledge and awareness of FEMA's Open Government initiative across the Agency and its whole community partners. Communications tools developed include internal intranet pages, a public email account, an IdeaScale campaign, public webpages, and the use of multiple social media channels to promote the initiative provide access to agency datasets, and provide an avenue for public feedback. At the closing of year one, OpenFEMA had:

- Established contacts with more than 60 external stakeholders (12 non-profits/associations/non-governmental organizations, 17 companies, 11 universities and 23 offices/programs at federal and government agencies). These numbers do not include contacts from FEMA or the rest of DHS.

- Received requests/questions related to open data through the OpenFEMA email account, which has led to the development of new datasets and external contacts.
- External stakeholders are referring their trusted partners to OpenFEMA. Numerous external entities and partners have been brought into the fold and are consuming FEMA data at the behest of current data consumers.

Making Big Data More Consumable Through Challenges:
The United States Fire Administration National Fire Incident Reporting System fire incident and cause data was large, complex, difficult to understand, and not easily accessible. In fact, the data was only available on CD-ROMs. OpenFEMA released the largest fire dataset in the world and made it available for access online, which allowed for the many external stakeholders to create fire data visualizations. External entities also used the data during a “civic hacking” event, resulting in the launch of six fire visualization tools that provide valuable insight to citizens, local governments, and first responders.

Updates to Previous Flagship Initiatives

FLAGSHIP: NATIONAL INFORMATION EXCHANGE MODEL

The National Information Exchange Model (NIEM) is a federally-supported, government-wide initiative that helps communities of people with common mission interests connect and exchange information in order to successfully and efficiently accomplish their missions.

By providing a common vocabulary and mature framework to facilitate information exchange, the model enables diverse communities to "speak the same language" as they share, exchange, accept, and translate information efficiently.

Instead of seeking a nationwide integration of all local, state, tribal, and federal information systems, NIEM focuses on the development of shared services using cross-boundary information exchange across multiple levels of government. In this way, NIEM breaks down agency stovepipes and creates the opportunity for agencies to share information quickly and effectively without rebuilding systems. All 50 states, the majority of federal agencies, including the Department of Defense, and the international community are committed to using the model in some capacity and at differing levels of maturity.

A grassroots initiative, NIEM was born as a best practice developed at the state and local levels of government. Today, the model is a national program with international adoption. The federal sponsors of NIEM include the Department of Justice, Department of Homeland Security, and Department of Health and Human Services.

The NIEM program has recently completed the following milestones.

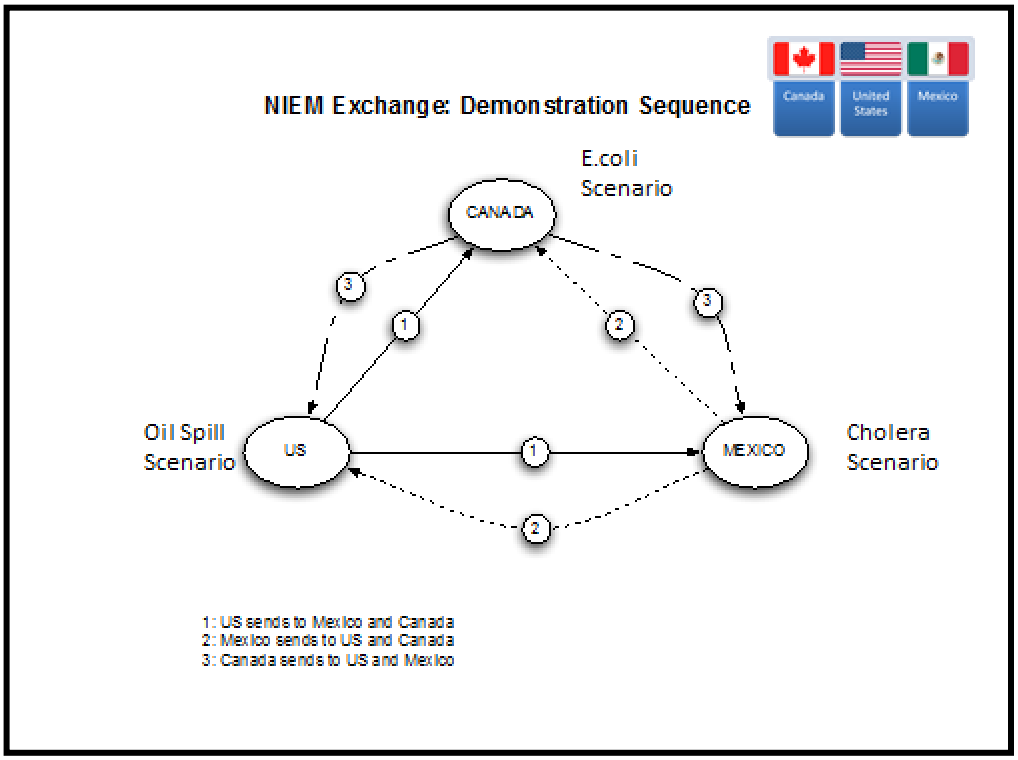
1. North America Day Working Group Charters

    a. The Public Health Working Group charter was established in January 2012 (**Milestone: Q4 FY 2013** / **Actual: Q2 FY 2012**).
    b. The Public Safety Working Group charter was established in January 2012 (**Milestone: Q4 FY 2013** / **Actual: Q2 FY 2012**).

2. Pilot exchanges

    a. Public Health:

    The working group successfully conducted a pilot demonstration of NIEM-based information exchange between U.S., Mexico, and Canada in August 2012. (**Milestone: Q4 FY 2014 / Actual: Q4 FY 2012**).


NIEM Exchange: Demonstration Sequence
Canada
United States
Mexico
E.coli Scenario
CANADA
Oil Spill Scenario
US
MEXICO
Cholera Scenario
1
2
3
1: US sends to Mexico and Canada
2: Mexico sends to US and Canada
3: Canada sends to US and Mexico

    b. Public Safety:

    The working group successfully conducted a pilot demonstration of stolen vehicle information exchange. All three countries were able to successfully connect and exchange test data using NIEM. (**Milestone: Q4 FY 2014 / Actual: Q4 FY 2013**).

For more information about NIEM, please visit www.niem.gov.

FLAGSHIP: OFFICE OF ACADEMIC ENGAGEMENT

The Office of Academic Engagement (OAE) was established to support the DHS mission by building, improving and leveraging relationships with the academic community. The office coordinates DHS academic policy; facilitates inter- and intra-agency coordination on academic affairs; markets and promotes DHS resources; and collaborates with students, faculty, and academic institutions.

The Department maintains numerous relationships with members of the academic community, who are reflected in OAE's focus areas: attracting talented students and recent graduates to careers at DHS; promoting academic research that addresses pressing homeland security needs; enhancing campus resilience and preparedness; supporting homeland security academic programs; and improving the international student immigration process. The office works across DHS Components and alongside agency partners including the Departments of State, Education and Justice to address each of these priority areas.

In addition, OAE manages the Homeland Security Academic Advisory Council (HSAAC), a DHS federal advisory committee comprised of prominent higher education leaders, including college and university presidents. The HSAAC is charged with advising the Secretary and DHS senior leadership on matters related to homeland security and the academic community. The HSAAC provides DHS and the public with a transparent vehicle to receive advice and recommendations directly from those impacted by DHS academic policies, programs, resources, and recruitment and workforce education efforts. Per the *Federal Advisory Committee Act*, all HSAAC meetings are open to the public and all meeting materials and minutes are posted on the HSAAC website.

The office also supports the *Study in the States* initiative in collaboration with U.S. Immigration and Customs Enforcement's (ICE) Student and Exchange Visitor Program. The *Study in the States* initiative expands public engagement between the government and academia, and provides an innovative website, http://studyinthestates.dhs.gov, that serves as a central online information hub for DHS and its agency partners to provide current and prospective international students with up-to-date information in a streamlined, dynamic, user friendly format. By streamlining all pertinent international student information into an interactive website, the *Study in the States* initiative allows DHS and its partner agencies to proactively coordinate and disseminate information to the more than 1.1 million international students, exchange visitors and their dependents that travel to the United States to study each year.

The following are completed deliverables:

- **Q2 FY 2014 –** Renewal of the HSAAC Charter
- **Q2 FY 2014 –** Public Meeting of the HSAAC

The following are planned deliverables:

- **Q3 FY 2014 –** Launch of the *Study in the States* mobile platform
- **Q1 FY 2015 –** Public Meeting of the HSAAC

III. New and Expanded Initiatives

Open Data

Enterprise Data Inventory

In compliance with OMB Memorandum M-13-13, DHS has developed the Enterprise Architecture Information Repository (EAIR); a centralized repository of Enterprise Architecture assets used by DHS and its Components. Each DHS Component is responsible for maintaining an accurate, up to date description of its data assets within the EAIR under DHS policy, and as documented in the Enterprise Data Management Concept of Operations. Progress on this initiative has been captured for the past four years on the Enterprise Data Management Scorecard, which is presented quarterly to the DHS CIO Council. Primary Enterprise Architecture assets contained within the EAIR include technology products and standards in the DHS Technical Reference Model, systems, services and data architecture elements.

Enterprise Architecture Information Repository

DHS has been populating the EAIR with extensive data asset metadata since 2008 and has been able to associate over 80% of its systems to a corresponding data asset. The EAIR currently includes approximately 800 data assets and several hundred datasets representing web pages and other shared data. The published data assets are now undergoing a registration and certification process to identify authoritative and trusted data sources. The intent of certifying a data asset as authoritative is to increase the reuse and confidence level in the data. In fiscal year 2014, DHS expanded the metadata profile of each data asset and dataset to include access level (Public, Public Restricted and Non Public) and a web address URL so that a Public Data Catalog could be automatically generated.

Clarification of terms:

A **data asset** is a distinct organized collection of structured, semi-structured or unstructured values. Examples include a database, web site, document repository, Excel spreadsheet, extended mark-up language (XML) file, a geospatial image file or a data service.

A data asset may produce or store one or more **datasets**. For example, the National Emergency Management Information System (NEMIS) - Emergency Support Module is a FEMA data asset. The FEMA Disaster Declarations Summary and the FEMA Hazard Mitigation Program Summary are two datasets extracted from NEMIS

The information in the DHS EAIR includes security classification, privacy sensitivity, and handling restrictions such as For Official Use Only, Law Enforcement Sensitive, Special Security Information and other types of Controlled-But-Unclassified categories including non-government restrictions such as data protected by trade agreements or those to protect intellectual propriety of private sector partners.   Because of its homeland security and national security missions, the categorization of the data assets shows that only 15 percent of the 800 data assets and datasets contain data that is releasable to the general public.

One of the primary purposes for the collection of the data asset metadata is to further the Department's information sharing mission by ensuring a broad, Department-wide understanding of DHS data. The Enterprise Architecture Information Repository is used to allow discovery of data being used at the Department, ultimately resulting in reuse and increased sharing across DHS and with its federal, state, local, tribal and private sector partners.

The Department expanded the purpose for collecting data asset and datasets to encompass the broader mission of data dissemination in addition to information sharing as part of the Open Government Initiative. Institutionalizing data dissemination to the public and creating a culture for Open Governments includes putting into place a process where each data asset owner within the Components will review each data asset and identify potential candidate datasets which could be served to the public via Data.gov.   This was added to the Enterprise Data Management Scorecard in 2013.   In this process, the data owners specify the broadest allowable scope for dissemination of the candidate dataset – the general public, private sector partners, state and local government, other federal government, and other DHS organizations.

This list of potential candidate datasets for dissemination to the public is put through the Department's Open Government Initiative review process to address legal, financial, privacy and security concerns with release ability, which results in the publishing of publically releasable data.   Of the 600 data assets and associated systems, approximately one half have been reviewed in FY 2014, resulting in a list of 75 datasets available on the Public Data Catalog.

In fiscal year 2014, an expanded Digital Strategy report will be updated quarterly to report status on the candidate data sets review/approval processes and submissions to Data.gov.

DHS relies on the EAIR approach because an official data inventory did not exist in any of its related Components that came together in 2002 to become DHS. The DHS systems inventory has changed several times over the past 5 years and now relies upon the official Federal Information Security Management Act inventory of systems. DHS reviews the completeness of its data asset metadata yearly and works with the Components to enrich the content where appropriate to make discovery more accessible and understandable. The data asset metadata profile was based on the Dublin Core (a recognized metadata standard) and consequently matches up well with the Data.gov common core. The DHS Enterprise Architecture program includes segment architecture efforts for each of the mission areas and includes data gathering efforts for the baseline and target data architecture. This approach has provided additional discovery of information product datasets supporting each of the mission areas. During FY 2014, the Enterprise Architecture program will be addressing at least 3 of our major missions and defining baseline and target architectures supporting those missions. The segment efforts should result in the identification of data assets and datasets which will be added to the Enterprise Data Inventory. Additionally, existing web pages will be reviewed to determine is additional dataset information can be captured and added to the Enterprise Data Inventory. Progress to support the enrichment of the DHS Enterprise Data Inventory will be reported on a quarterly basis and presented to the major DHS collaboration groups in order to improve support of data gathering efforts. This approach was successfully employed with the initial data gathering effort of the Enterprise Data Repository. The progress report along with the Public Data Catalog will be updated on the DHS Digital Strategy web page so the public can be informed.

Challenges/Solutions:

Web publishing is one of the biggest challenges the Department faces in registering datasets. Many Components do not have readily available server space that may be accessed from outside of DHS; therefore web pages become the de facto solution. The DHS OCIO and Components are working to identify potential solutions to this problem. The Data.gov Program Management Officer (PMO) is providing hosting space for datasets on the new Socrata platform that was released in December 2011. DHS will use this option as part of the new Safety.data.gov community data sets and consider this alternative as more service details become known. FEMA has developed a new document management approach that may provide an answer to reducing the number of separate web pages being created and maintained by using a combination of publicly accessible data storage and application program interfaces.

Another major challenge for DHS is the need to protect sensitive information. Protecting sensitive information is critical to the work of the Department, and as such is a deeply rooted part of the DHS culture. DHS is striving to balance the need to safeguard sensitive information and the responsibility to disclose valuable information to the public. The Department has established a collaborative review process to ensure that the data provided informs the public without compromising security or privacy. This review process currently takes an average of two months per dataset, depending on the questions that arise in the review.

During the review process, the Department identified datasets that were determined not releasable due to the sensitivity of the information in the reports. Many of these datasets are suggestions received from the general public.

Below are examples:

Dataset	Component	Rejection Reason
HSIP Freedom Geo-layers (160+)	National Protection and Program Directorate (NPPD); OCIO	Contains "For Official Use Only" (FOUO) data essential to the value of the dataset; identified a solution to facilitate proactive planning and preparations by State/Local/Tribal/National users only who meet the FOUO classification; still deemed inappropriate for the public.
Merchant and Recreational Vessels	USCG	Deemed Inappropriate by Privacy Office; Resubmitting with Redacted information for review.
Border Encounters	CBP	Contains "For Official Use Only" and personally identifiable data. Restrictive access to qualified research organizations.

Candidate datasets are identified in a number of ways. First, the Department nominated a set of high value datasets as candidates for publication on Data.gov. These candidate datasets were initially the primary focus and the starting point for identification of the DHS candidate pipeline. They provided an example of the kind of Department information that would be considered high value that could guide the Components in targeting additional candidates.

Then Components self-nominated datasets they could contribute. Suggestions have also been received from the Data Management Working Group and Web Council. OCIO identified data that is already published by the Department through Component websites, which can be provided in a more open, usable format. OCIO is documenting this data in the Enterprise Architecture Information Repository where DHS employees can view the public data catalog pipeline and make additional suggestions.

Most importantly, suggestions are provided by the general public through the Data.gov public forum. These suggestions are provided to DHS through the Data.gov program management office. When suggestions for information deemed to be too sensitive for release are received, Components strive to see if the data can be modified such that it is releasable and still useful.

The DHS OCIO identifies potential sources for the candidate datasets and collects some high level information to determine whether or not the dataset is eligible for release. This high level summary answers four basic questions:

- What is the data in the submission?
- How is it generated?
- How can the data be used?

- What data types will be in the dataset?

The DHS OCIO works with the organization that maintains the source system for the data to determine the level of effort that would be required to produce the dataset.

The DHS OCIO will continue to develop and provide training materials to promote awareness of Data.gov across the Department programs. The training provides an introduction to the Open Government Initiative and the concepts surrounding Data.gov. The training will be targeted toward DHS program managers, who are ultimately the business stewards of the data specific to their program. Program managers will be asked to identify candidate datasets that could be produced from their programs.

Public Data Catalog

A public data listing is available in the DHS section of Data.gov. DHS has added several new metadata fields to the Enterprise Data Inventory to allow the public data catalog to be extracted along with the data.gov metadata. A public access metadata field contains a drop down for Public, Public-Restricted, and Non-Public. A second metadata field provided for a reason text if the first field is Non-Public or an URL when available, if the first field value is Public. All data assets and datasets marked Public and Public-Restricted in the DHS Enterprise Architecture Information Repository are extracted when the Public Data Catalog extract script is executed monthly or on the quarterly milestone date. The Public Data Catalog is updated with the Agency and Program values for each extracted row and converted to JSON. The Data.JSON file is then published on the DHS Digital Strategy web page.

The Under Secretary for Management (USM) and the DHS Chief Information Officer (CIO) continue to work with the Components, the Data Management Working Group, and the Open Government Working Group to promote Data.gov candidate submission and review processes within the Components. These processes are coordinated through the Office of the Chief Information Officer and include the collaborative review by Privacy, Security, Office of General Counsel, USM, and the Enterprise Data Management Office.

OCIO continues to develop materials to educate DHS employees about the Data.gov and promote awareness and participation. OCIO is also institutionalizing participation in Data.gov as part of a larger effort to incorporate data dissemination consideration into the Systems Engineering Life Cycle and the DHS culture. DHS has incorporated guidance and decision points into the engineering life cycle that encourage programs to consider all of the potential audiences and users of the data in a particular system and incorporate the process for data dissemination over the life of the system. Investment submissions are reviewed each year to determine if data dissemination is being addressed or improved.

For additional information, please visit: http://catalog.data.gov/organization.

S & T Office of University Programs – Cooperative Research efforts

In support of the focus on collaboration as defined by the Open Government Directive, the Office of University Programs in the Science and Technology Directorate has several Centers of Excellence that routinely work with DHS Components on developing analytical products and tools to improve the mission capabilities and efficiencies of DHS Components. This effort is closely monitored by the Directorate to ensure that data is adequately protected and used according to the Cooperative agreement or Basic Ordering Agreement (BOA). Managed through the Directorate's Office of University Programs, the COEs organize leading experts and researchers to conduct multidisciplinary homeland security research and education. Each center is university-led or co-led in collaboration with partners from other institutions, agencies, national laboratories, think tanks and the private sector. Datasets being used for these efforts are considered Public Restricted as they require Non-Disclosure agreements and information sharing plans in order for the researchers to gain access to sensitive Component data.

For additional information, please visit: http://www.dhs.gov/st-centers-excellence.

Proactive Disclosure

In order to support the Open Government Directive, the Privacy Office has taken the lead on providing guidance for proactive disclosure of information. The Privacy Office maintains its commitment to transparency through the continued reduction of FOIA backlogs and increasing transparency through accessibility. Successes in open government for the Privacy Office include electronic reading rooms within DHS operational Components, and a significant reduction in backlogged FOIA requests. The Freedom of Information Act outlines the transparency requirements government agencies must follow. The DHS FOIA Office is responsible for proactively posting documents related to headquarters activities outside of the Privacy Office, and coordinates with headquarters offices in order to continue to update the FOIA Electronic Reading Room. The FOIA Office also coordinates with and assists the Components in their efforts to comply with the *Proactive Disclosure Memorandum* dated August 2009.

Under the leadership of the Chief FOIA Officer and Chief Privacy Officer, DHS is proactively disclosing several categories of records on its agency websites and links to their respective electronic reading rooms. Due to the continued increase of proactively disclosed documents in the DHS FOIA Electronic Reading Room, the FOIA Office has worked diligently to enhance its FOIA Electronic Reading Room to better accommodate its robust collection of documents.

The following are Proactive Disclosure types:

- Historical daily schedules of the most senior agency officials (notated to reflect that officials may have deviated from the posted schedule and abridged as appropriate for security and privacy concerns);

- Executed contracts and grants;
- Management Directives and instructions;
- Congressional logs and correspondence under DHS control;
- FOIA logs
- Any records released pursuant to a FOIA request that have been, or are likely to become, the subject of three or more requests.

The following are Privacy types:

- Annual Privacy Report of Congress
- All Privacy Impact Assessments
- System of Records Notices
- Privacy Compliance Review
- Quarterly Privacy Reports
- Data Mining Reports

The DHS FOIA library can be found here: http://www.dhs.gov/foia-library

Each component of DHS has been tasked with identifying records that should be proactively disclosed on their website. Here are some examples of proactive disclosure efforts at DHS Components:

Federal Law Enforcement Training Center (FLETC):

- FLETC tracks frequently requested records – per DOJ guidance and reviews records for potential posting due to considerable public interest.

The FLETC library can be found here: http://www.fletc.gov/reference/public-information/freedom-of-information-act-foia/reading-room.

U.S. Immigration and Customs Enforcement:

- Secure Communities Nationwide Interoperability Statistics;
- Office of Detention Oversight Compliance Inspection Reports;
- FOIA Logs;
- Student and Exchange Visitor Program Quarterly Reports and Statistics;
- Testimony of former Dir. John Morton before the House Judiciary and Appropriations Committees; and
- Prosecutorial Discretion policy memoranda.

The ICE FOIA library can be found here: http://www.ice.gov/foia/library/index.htm

Operations Coordination and Planning:

- OPS evaluates records using the criteria of whether the records have been requested multiple times by different sources, whether they are related to a current event and likely to be requested again, or whether they are related to similar requests from previous years, e.g., a specific set of statistics requested each fiscal year by multiple sources. If OPS determine that records meet the aforementioned criteria, OPS posts the records in the DHS reading room.

Privacy Office/FOIA Office:

- In the new software tracking system, an electronic monitoring, tracking and redacting commercial off- the- shelf web application, DHS is now able to determine key words associated with each request and enter them in FX under the “Other Information” tab; scroll down on that tab and enter the key words in the “Keywords ‘a2d’ Purposes” box.

Selecting Keywords to Help Identify Frequently Requested Records - Help Implementing (a)(2)(D) of the FOIA

STEPS	1. Read description and identify records requested.	2. Identify Keyword related to Documents Requested with help from Chart below. Do not select keyword based on background information given in request.	3. Enter Keyword into (a)(2)(D) Keyword field in FX

Single Keyword

Request Type	Examples - Documents Requested	Keyword	Notes
Contract # /Grant #	Contract HSBP1004C00193	HSBP1004C00193	If an umbrella contract, list the subcontracts underneath umbrella too
Report or Investigation Name	FPS Investigation Report #0003	FPS Investigation Report #0003	Specific Document Requests such as policies, reports or investigations
DHS Program Titles	See Something, Say Something related emails	See Something, Say Something	
	ATS -Automated Targeting System - All Records	Automated Targeting System (ATS)	
	CFDA DHS 97.065 - Budget info 2011-2013	CFDA DHS 97.065	
Document Type	S1 Calendar - Napolitano	Napolitano - Calendar	
	S1 Meeting with Mexican Govt in 2012	Napolitano - Mexico Meeting	
	Credit Card List 2012	Credit Card List	
	Border Arrest Statistics for Arizona in 2012	Border Arrest Statistics	
	All New Immigration Reform Policy in 2013	Immigration Reform Policy	
	All DHS memorandums with USPS	USPS memorandum	
Major Events	all correspondence related to Boston Marathon	Boston Marathon	Boston Marathon, DeepWater Horizon, Occupy Wall Street
Correspondence - Congressional	Peter King Correspondence 2012	Congressional Correspondence - Peter King	Name Congressman and Date Range
Correspondence - Emails for DHS Employee	Amy Schlossman emails January 15, 2013	Correspondence - Amy Shlossman	
Own Records	All Record Contained in Afile regarding me	Personal Record	Code All Privacy Act requests as Personal Record.
	My Security File - John Smith	Personal Record	
	All my records	Personal Record	
Other Search Terms/Topic	Chemical Waste Company monitoring	Chemical Waste Company	Company Names
	Automatic license plate reader - All Policy Docs and handbooks	Automatic license plate reader	
	Human Trafficking Statistics 2012 Arizona	Human trafficking statistics	
	Admin file for DHS PRIV FOIA case 2013-HQFO-99887	2013-HQFO-99887	

Two or More Keywords (Separate two Keywords by semi-colon)

Request Type	Examples - Documents Requested	a2d Term	Notes
Correspondence - Congressional - Major Event	All Peter King Correspondence to DHS regarding Boston Marathon bombings	Boston Marathon; Congressional Correspondence - Peter King	
Correspondence - Emails for DHS Employee - DHS Program	All emails between Amy Schlossman regarding Boston Marathon	Boston Marathon; Correspondence - Amy Schlossman	

U.S. Citizenship and Immigration Services (USCIS):

USCIS completed the Electronic Reading Room re-design in 2012 and identified a base set of categories believed to be of public interest. This list is reviewed and additional categories added from time to time.

- EB-5 Regional Centers
- Human Trafficking
- Adoptions
- A-Files of Interest
- USCIS Contracts
- FOIA Annual Reports
- FOIA Logs
- Administrative Appeals Office (AAO) Decisions
- USCIS Employee Information
- Employee Rights
- E-Verify
- SAVE
- Refugee, Asylee and International Operations Information
- Employment-Based Petitions
- Defense of Marriage Act (DOMA)
- Deferred Action for Childhood Arrivals
- Policies and Manuals
- Genealogy

USCIS FOIA Office works to proactively disclose records by taking the following steps: (1) Receive similar requests for documents at least three times; (2) Receive a request and determine its potential for public interest; (3) Identify certain records for immediate posting, such as FOIA Logs and Annual Reports; and (4) Ensure future plans include working its Significant Interest Groups to identify possible records for posting.

The USCIS FOIA library can be found here: http://www.uscis.gov/about-us/electronic-reading-room.

Use-of-Force Policies

In March 2014, CBP and ICE released their existing Use-of-Force policies to the public – established in 2010 and 2004 respectively. DHS is also making the overarching Department policy, established in 2004, publicly available.

> "Since I took office as Secretary of Homeland Security, I have been very interested in the issue of use-of-force by our agents and officers in the field. As I said earlier this year, transparency is essential to the credibility of a law enforcement agency within the communities it operates. This is why I am pleased that Customs and Border Protection, along with Immigration and Customs Enforcement, are delivering on a commitment I made in January and today are publicly releasing their use-of-force policies."
> *– Secretary, Jeh Johnson*

The policy is intended to create a uniform standard and provide guidelines for law enforcement officers and agents across the Department.

To view the use-of-force polices, please visit http://www.dhs.gov/publication/use-force-policy.

Privacy

DHS was the first agency to appoint a Chief Privacy Officer to ensure technologies used do not violate privacy protections, personal information contained in Privacy Act systems of record adhere to the Privacy of 1974, and to evaluate legislative and regulatory proposals involving collection, use, and disclosure of personal information by the federal government.

The Privacy Office accomplishes its mission by focusing on the following core activities:

- Requiring compliance with federal privacy and disclosure laws and policies in all DHS programs, systems, and operations;
- Centralizing Freedom of Information Actand Privacy Act operations to provide policy and programmatic oversight, to support operational implementation within the DHS components, and to ensure the consistent handling of disclosure requests;
- Providing leadership and guidance to promote a culture of privacy and adherence to the Fair Information Practice Principles (FIPPs) across the Department;
- Advancing privacy protections throughout the federal government through active participation in interagency fora;
- Conducting outreach to the Department’s international partners to promote understanding of the U.S. privacy framework generally and the Department’s role in protecting individual privacy; and,
- Ensuring transparency to the public through published materials, reports, formal notices, public workshops, and meetings.

For additional information, please see the Annual Privacy Report to Congress: http://www.dhs.gov/sites/default/files/publications/2013-dhs-privacy-office-annual-report-final-11062013.pdf

Whistleblower Protection

The Department is committed to protecting the rights of whistleblowers. The Department has taken several steps to codify this commitment in policy and is taking further steps as outlined below.

Protecting Government Contractors

The Whistleblower Protection Act required the Department to update nondisclosure agreements that are signed by contractors. DHS requires contractor employees to sign the DHS Form 11000-6 when the employee has access to DHS IT systems and in other special circumstances. DHS operationalizes this requirement using DHS Form 11000-6 which lets employees know that disclosures pursuant to illegality, waste, fraud, abuse, public health or safety threats are not barred by the form.

Protecting Employees with Access to Classified Materials

Presidential Policy Directive 19 ensures that employees serving in the intelligence community or who otherwise have access to classified information can report waste, fraud and abuse while protecting national security information. Further, the Directive prohibits retaliation against employees for reporting fraud, waste, and abuse. Specific accomplishments and plans include:

- The Personnel Security Division within the Office of the Chief Information Officer coordinated efforts with the Office of General Council to develop a revised Notice of Determination letter template including PPD-19 language for use throughout the Department. This template was distributed to Components in September 2013.
- The Personnel Security Division is updating the DHS Instruction 121-01-007 “Personnel Security and Suitability Program” to include PPD-19 language and procedure. This Instruction provides Department policy and guidance to headquarter and operational Component personnel security offices. The expected completion date is the end of Q4 FY 2014.

Protecting Employees

The Department provides information to employees about their rights as a whistleblower in a decentralized manner. To ensure that the information provided is current and consistent with best practices, the Department is pursuing efforts to qualify for Office of Special Council Certification. The Department will take the following steps to attain this Certification:

1. The Management Directorate’s Office of Public Affairs will establish an intranet site that shares information from the Office of Special Council on whistleblower protections and other areas under their jurisdiction.
2. The Chief Human Capital Officer will adopt the OSC promotional materials and distribute it to employees through the Human Capital Leadership Council. In addition, the Office of General Council will distribute the materials to the Chief Councils for their reference as well.
3. The Chief Human Capital Officer will provide training materials to supervisors either directly or through the Human Capital Leadership Council.

Websites

To comply with the 2014 Open Government Plan Guidance Memorandum to federal agencies, links to the following websites are provided below:

- **Digital Strategy Website: https://www.dhs.gov/dhs-digital-strategy**
- **DHS.gov Website Metrics: http://www.dhs.gov/sites/default/files/publications/February-2014-Metrics-DHS-v2.gov_.pdf**
- **Examples of commonly sought-after information:**
  1.“Check Immigration Case Status”
  2.“Careers”
  3.“Trusted Traveler Programs”

DHS has taken steps to make commonly sought-after information more accessible to the users by creating links on primary landing pages, short-cuts under a “How do I?” tab, and a search function on the header of each page. DHS will continue to analyze website metrics to ensure necessary links and short-cuts are available for commonly sought-after information.

IV. Ongoing Initiatives at DHS

Participation in Transparency Initiatives

In support of promoting transparency, DHS continues to participate in the following government-wide initiatives.

Data.gov

DHS is committed to safeguarding sensitive information while promoting a culture of information sharing and considering all high value data for release to:

- the general public and interested developers;
- state, local, tribal, and federal partners;
- university and research programs; and
- other DHS Components and programs.

DATA.GOV

DHS OCIO is also working with the Components, the Data Management Working Group, Web Council, and the Open Government Working Group to establish Data.gov candidate submission and review processes within the Components. FEMA and ICE have both established a Data.gov lead to facilitate their own Data.gov pipeline processes. These processes are coordinated through the OCIO and still include the collaborative review. FEMA also established the OpenFEMA initiative to actively promote data transparency for high value data and collaborate with the public and developers to expand the usefulness of their data. The Department is committed to providing the public with high value data while safeguarding sensitive information necessary to meet the mission of DHS.

For additional information, please visit http://www.data.gov.

E-Rulemaking

Federal regulations have been available for public comment for many years, but people used to have to visit a government reading room to provide comments. Today, the public can share opinions from anywhere on Regulations.gov.

Regulations.gov removed the logistical barriers that made it difficult for a citizen to participate in the complex regulatory process, revolutionizing the way the public

regulations.gov
Your Voice in Federal Decision-Making

can participate in and impact federal rules and regulations.

It provides citizens, small businesses, educators, corporations, civic organizations, and all levels of government one-stop internet access to view, download, and submit comments on all federal regulations currently under review. DHS accepts electronic submissions via the website and ensures public regulatory dockets are electronically accessible and searchable using Regulations.gov.

DHS is committed to supporting the E-Rulemaking initiative, thereby improving the public's access to and participation in the federal regulatory process. Through public involvement, the Department firmly believes the rulemaking process will become more efficient and effective.

For additional information, please visit http://www.regulations.gov.

IT Dashboard

The IT Dashboard is a website enabling federal agencies, industry, and the general public and other stakeholders to view details of federal information technology investments.

The purpose of the Dashboard is to provide information on the effectiveness of government IT programs and to support decisions regarding the investment and management of resources. The Dashboard is now being used by the Administration and Congress to make budget and policy decisions.

IT DASHBOARD

In support of promoting transparency, DHS is currently reporting information on 88 Major IT investments on a monthly basis.

For additional information, please visit https://www.itdashboard.gov.

Recovery.gov

Recovery.gov was created by the American Recovery and Reinvestment Act of 2009 to display information about the Recovery Accountability and Transparency Board's activities, as well as data related to the $840 billion stimulus bill and information about the distribution and spending of Hurricane Sandy funds.

RECOVERY.GOV
The official U.S. Government website for the Recovery Accountability and Transparency Board.

As part of H.R. 152, Congress authorized the Recovery Accountability and Transparency Board to "develop and use information technology resources and oversight mechanisms to detect and remediate waste, fraud, and abuse" in the awarding and spending of the funds. The Board is collecting data on entities being awarded contracts, grants, and loans and will display this data as it is collected.

DHS participates in Recovery.gov by providing information about “Where the money is going.” For example, Public Assistance funding for the Hurricane Sandy program provided by FEMA can be found here:

http://www.recovery.gov/Sandy/whereisthemoneygoing/Pages/DisasterReliefPrograms.aspx

CFDA.gov

The Catalog of Federal Domestic Assistance is a government-wide compendium of federal programs, projects, services, and activities that provide assistance or benefits to the American public. It contains financial and nonfinancial assistance programs administered by departments and establishments of the federal government. Currently, DHS has 85 programs listed in the CFDA.

There are several important data elements in the CFDA that are updated annually and reviewed by OMB. The required data elements are as follows:

- **Program Authorization** – cite the appropriation authorization for the program;
- **Program Objective** – relate to the Presidential Policy Directive (PPD-8) National Preparedness, Security, Resilience, Prevention, Mitigation, Response, Protection, and Recovery;
- **Program Obligation** – include three years of financial obligations (Past-Actual, Present - Estimate, Future - Estimate);
- **Unique Treasury Appropriation Fund Symbol** (TAFS) – include a 2 digit Department Code, and 4 digit Treasury Account Main Code;
- **Program Accomplishments** – include three years of program accomplishments (Past-actual, Present-estimate, Future-estimate)
- **POC** – provide name, number, and address of subject matter expert of the program is provided

For additional information, please visit https://www.cfda.gov.

Grants.gov

Grants.gov provides a single website to find and apply for federal discretionary grants. Grants.gov provides over one million organizations a single web site where they can find and apply for over $153 billion worth of grants distributed annually. It empowers smaller agencies with limited resources to improve

GRANTS.GOV℠

FIND. APPLY. SUCCEED.℠

the reach of their grant programs, and provides larger agencies with the benefit of process standardization, cost savings, and increased visibility. The program is funded by the 26 federal grant-making agencies, including DHS, each providing support commensurate with its size according to a formula approved by the Council on Financial Assistance Reform (COFAR).

In FY 13, DHS posted over 80 funding opportunity announcements on Grants.gov. These opportunities resulted in approximately 7000 awards to a total of almost 5000 grant recipients representing about 71 different grant programs listed on the CFDA. Total grant dollars awarded in FY 13 were approximately $7 billion. While all federal grant opportunities are required to be posted on Grants.gov, not all DHS applications are submitted through that venue. FEMA collects some submissions through specific grants management systems, such as the E-grants Application System and the ND Grants System.

For additional information, please visit http://www.grants.gov.

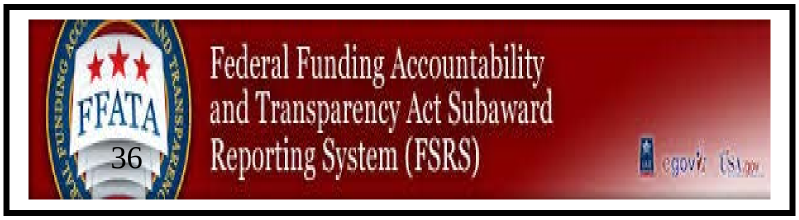
SAM.gov

The System for Award Management (SAM) is the Official U.S. Government system that serves as the entry point for prospective federal contractors and grant recipients. SAM was created to simplify the often onerous task of finding information about contracts and grants and being properly registered as a federal recipient to apply for a federal award. SAM combines several systems into one, thus improving the federal contractor and grant recipient experience. The first phase of the consolidation brought the Central Contractor Registry; the Federal Agency Registration; the On-line Representations and Certifications Application; and the Excluded Parties List System into SAM. Future phases of the SAM consolidation include absorbing the Catalog of Domestic Assistance and federal procurement systems.

For additional information, please visit https://www.sam.gov.

FSRS.gov

Increasing transparency and improving access to federal Government information, particularly information on federal spending, is a primary objective of Open Government. The *Federal Funding Accountability and Transparency Act* (FFATA) was amended by the Government Transparency Act of 2008


FFATA
FEDERAL FUNDING ACCOUNTABILITY AND TRANSPARENCY
Federal Funding Accountability
and Transparency Act Subaward
Reporting System (FSRS)
egov
USA.gov

(Public Law 110-252) requiring disclosure of additional information from recipients and information on first-tier sub-recipients on new awards on or after October 1, 2010.

The FFATA Subaward Reporting System (FSRS) is the reporting tool for federal prime awardees (i.e. prime contractors and prime grants recipients) use to capture and report subaward and executive compensation data regarding their first-tier subawards to meet the FFATA reporting requirements. The CFO's Office for Financial Assistance Policy and Oversight (FAPO) provides guidance and support to the various financial assistance awarding Components in ensuring this requirement is understood and fulfilled. Also, FAPO provides training sessions regarding the importance of accurate and timely FSRS reporting directly to the applicant community as well as to DHS Components that award financial assistance.

USAspending.gov

The Federal Funding Accountability and Transparency Act of 2006 requires that the Office of Management and Budget establish a single searchable website, accessible to the public at no cost, which includes detailed information for each federal award.

In support of the promoting accountability and transparency, DHS participates by posting financial data to USAspending.gov. The Department's Office of the CFO will continue to assess quarterly the accuracy, completeness, and timeliness of data posted to USAspending.gov, the main portal for financial data on government contracts and financial assistance awards. In 2012 OMB released a memorandum on Improving Data Quality for USAspending.gov. This latest guidance requires agencies to do the following:

- Assign a Financial Assistance Identifying Number unique to each financial assistance award and to be maintained during life of award.
- Develop and implement procedures to validate USAspending.gov prime federal award financial data with data maintained in the agency's financial system.
- Report to OMB the accuracy rate of USAspending.gov prime federal award financial data within 60 days of close of each quarter
- Provide assurances for that the prime federal award financial data reported on USAspending.gov is correct at the reported percentage of accuracy, and the agency has adequate internal controls over the underlying spending.

The Department has developed the following milestones to ensure data quality of the data reported on USAspending.gov:

Milestones to support the accuracy, completeness and timeliness of all financial assistance data posted to any public venue	**Finish Date**
Conduct monthly meetings with the Financial Assistance Reporting Working Group to discuss emerging issues	Recurring
Identify a Financial Reporting Accountable Official for each Component	Completed: October 2010
Develop standard model for reporting /New Access Reporting Tool/Exception Reports on posted USAspending data	Completed April 2014:
Bring DHS closer to compliance with FFATA requirements.	In Progress
Develop business models and business rules related to reporting for the DHS-wide enterprise system.	In Progress

Table 1 – Data Integrity Milestones

The Department has released written guidance, formed working groups, provided Component support tools, and created a financial assistance inventory in assessing and improving USAspending data quality.

Financial Management Division's Component Requirement Guide provides the Components with a written policy and procedures to assess the data quality of the financial information in USASpending.gov. These procedures provide a means to determine completeness by reconciling total obligations calculated in the Statement of Budgetary Resources and/or appropriate aggregated United States Standard General Ledger accounts from the Department's financial management system-of-record to USASpending.gov data. The Components are required to perform a comparison at the transaction level to test accuracy and timeliness for data posted to USAspending.gov. If any of these metrics for completeness, accuracy, or timeliness falls below 95%, Components are required to supply Corrective Action Plans to the division. This process has been in place and is reviewed annually since FY 2011. Starting in 2014, these results are reported to OMB on a quarterly basis.

Starting in FY 2013, FM began performing annual sample testing of financial assistance data in USASpending.gov against source documentation to test other key qualitative attributes beyond obligation amount. The sample testing along with the quarterly reconciliations will be the basis for the FY 2014 assurances over prime award data in USAspending.gov.

The Department's Financial Management Division established the Data Quality Working Group (DQWG) in FY 2011. Members represent every Component's financial management community, the Financial Assistance and Policy Oversight (FAPO) branch, and the Office of the Chief Procurement Officer. The DQWG meets as needed to discuss best practices, lessons learned, common corrective action plan implementation, future data quality consideration, and methods to improve efficiency.

To improve accuracy and efficiency in measuring data quality, the Department has and is continuing to develop tools to assist our efforts. Current tools are the financial management systems to USAspending.gov data reconciliation template and the Department's progress tracking dashboard.

FAPO hosts the Financial Assistance Reporting workgroup. This workgroup is attended by financial assistance personnel in the areas of program, policy, and finance, including DHS Chief Financial Officers. The workgroup regularly discusses a variety of financial assistance topics including the need for the CFO's to certify financial assistance data on a regular basis. Impeding progress on certification on the timeliness, accuracy, and completeness of the data includes lack of financial assistance reporting systems. Data for USAspending must be manually collected for certification. The manual process is labor intensive and prone to errors.

The Department recently developed a new Access Tool to submit all its USAspending data. This tool has additional validation checks build into it which makes the data submitted more accurate. Also, the Department developed Exception Reports that identifies errors on existing posted USAspending data. All the inconsistent data is then corrected to make the data posted on USAspending more accurate.

Beginning in FY 2011, FAPO created and maintains a financial assistance inventory. This inventory includes data obtained from multiple sources including CFDA.gov, Funding Opportunity Announcements, USAspending.gov data, congressional notifications and Component award notifications. The inventory discloses a wide variety of spending and award information, highlighting gaps in financial assistance reporting data due to the fact the Department has no Department-wide grants management reporting system.

FAPO created a Financial Assistance Annual Report beginning in FY 2012. The purpose of the Report is to provide information on financial assistance programs administered across DHS Components. The Report provides information on the types of financial assistance, programs, funding by Component, the USAspending.gov Data Quality Plan, and audit requirements of financial assistance.

OCFO will continue to assess the completeness, accuracy, and timeliness of data posted in USASpending.gov; in addition, OCFO will continue to work with Components to achieve the Department's goal of 100% completeness, accuracy and timeliness of the data posted.

For additional information, please visit http://www.usaspending.gov.

Public Notice

The Department informs the public of significant activities and business by providing advisory committee information to the publicly accessible Federal Advisory Committee Act (FACA) database

In compliance with FACA Implementing Regulations (41 CFR 101-6 and 102-3), FACA groups are subject to the following requirements:

- Open, pre-announced meetings;
- Public access to discussions, deliberations, records and documents;
- Opportunity for the public to provide written (and often oral) comments;
- Fairly balanced membership; and,
- The evaluation of conflicts of interest for certain members.

Access to the government-wide FACA database is available at: http://www.facadatabase.gov.

In addition, the Department publishes a Federal Register Notice for the following entry types:

- Presidential Documents, including Executive orders and proclamations.
- Rules and Regulations, including policy statements and interpretations of rules.
- Proposed Rules, including petitions for rulemaking and other advance proposals.
- Notices, including scheduled hearings and meetings open to the public, grant applications, administrative orders, and other announcements of government actions.

For additional information, please visit https://www.federalregister.gov and http://www.dhs.gov/news.

Records Management

DHS recognizes the integral role Records Management plays in supporting DHS mission activities, promoting transparency to the public and ensuring greater information sharing across the federal government. DHS is actively working to meet the requirements outlined in the President's November 28, 2011 *Memorandum on Managing Government Records* and the accompanying August 24, 2012 *Managing Government Records Directive*.

Over the past year, the Department collaborated with the legal and Freedom of Information Act lines of business to build stronger Information Governance across the enterprise. The Department is exploring options for creating a Department-wide eDiscovery and Electronic Records Management System (ERMS). This will enable the Department to automate many currently manual processes, provide the technology to manage all electronic records in their native format and ensure compliance with requirements outlined in the Managing Government Records Directive.

DHS is tracking all of its unscheduled records. The Department is committed to ensuring all of these records are scheduled and maintained in accordance to the National Archives and Records Administration (NARA) approved retentions. The Department is providing quarterly updates on the scheduling progress to the appointed Senior Agency Official (SAO). In addition, efforts are being taken to transfer records over 30 years old with long term retentions to a NARA approved facility. The United States Secret Service completed the transfer of records last year and the United States Coast Guard will complete their transfer of records this coming year.

Freedom of Information Act (FOIA) Requests

The DHS FOIA Office is part of the DHS Privacy Office. The FOIA is a federal statute that generally provides that any person has a right to request access to federal agency records.

The Secretary of Homeland Security designated the DHS Chief Privacy Officer to serve concurrently as the Department's Chief FOIA Officer to promote efficiency, effectiveness, and statutory compliance in administering the FOIA. Capable and customer oriented FOIA operations play a huge role in the Department's efforts to promote transparency while fulfilling its mission. The Chief Privacy Officer leads the DHS Privacy Office (Privacy Office), and reports directly to the Secretary on both FOIA and privacy-related issues.

The Privacy Office ensures overall compliance with FOIA by developing Departmental policy needed to implement important FOIA initiatives, such as the sweeping changes set forth in the President's FOIA Memorandum and the Attorney General's FOIA Guidelines of 2009. Additionally, the Privacy Office performs coordination and oversight of Component FOIA operations, provides FOIA training, and prepares mandated annual reports of the Department's FOIA performance. The Privacy Office, through its FOIA unit (hereinafter referred to as the DHS FOIA Office), also processes initial FOIA and Privacy Act requests to the Office of the Secretary (including the Military Advisor's Office and the Office of Intergovernmental Affairs), and eight DHS headquarters Components (DHS FOIA Office Components).

Timely publication of information is vital, and the Department does not view delays as an inevitable and insurmountable consequence of high demand. The Department has shifted its focus from by-request FOIA services to a more proactive approach for sharing information. The FOIA website hosts detailed information on how DHS processes requests, details how to submit a FOIA request, and links to the FOIA Electronic Reading Room. By policy, DHS affords all individuals the same rights of disclosure under the Privacy Act as statutorily granted to U.S. citizens. This provides the maximum allowable disclosure of agency records upon request.

Record Setting FOIA Requests

DHS received more FOIA requests than any other federal agency in each of the last two fiscal years (2012 and 2013). In FY 2012 DHS received a record-setting 190,589 requests and processed 205,895 requests to reduce its backlog of pending requests from 42,371 to 28,553. In FY 2013, DHS received another record breaking number of FOIA requests - 231,534. While DHS processed 208,326 records in 2013, an increase over 2012, the backlog nevertheless increased to 51,761 due in part to the unprecedented number of requests received.

In 2013, the DHS FOIA Office implemented a new electronic monitoring, tracking and redacting commercial off the shelf web application solution to streamline the processing of requests and appeals under FOIA and the Privacy Act of 1974.[1] As a result of implementing the new application, DHS has seen numerous benefits such as: (1) increased productivity; (2) enhanced accuracy in reporting statistics, tracking cases, and better data integrity; and (3) improved interoperability and standardization of the FOIA process across the Department.

The volume of requests the Department receives may be due in large part to the interest of the public in DHS's mission and the function of its components. Of particular interest to the public are immigration-related records under the purview of U.S. Customs and Border Protection , U.S. Immigration and Customs Enforcement, the Office of Biometric Identity Management within the National Protection and Program Directorate, and U.S. Citizenship and Immigration Services. These components continue to receive the largest number of requests, receiving 97 percent of all requests in FY 2013.

The DHS Privacy Office remains committed to promoting transparency in DHS operations through timely and thorough processing of FOIA requests, reducing its backlog, and providing gold standard customer services and support.

For more information regarding DHS FOIA operations and processes, see the DHS Privacy Office 2014 Chief FOIA Officer Report:

http://www.dhs.gov/publication/chief-foia-officer-report-2014.

Congressional Requests

The Department values communications with Congress as a central tenet of its open government efforts. The Office of Legislative Affairs provides briefings, testimony, background information, staff discussions and field visits for Congressional members for a better understanding of DHS operations. OLA communicates accurate and detailed information to congressional interests, while following appropriate protocols to safeguard classified or otherwise sensitive information.

For additional information, please visit http://www.dhs.gov/about-office-legislative-affairs.

Declassification of Department of Homeland Security Information

Only in existence since 2003, the DHS has a minimal number of records of permanent historical value that are subject to the automatic declassification provisions of Executive Order 13526, “Classified National Security Information.” The majority of these records were produced by legacy components of DHS, which include the United States Secret Service (USSS), the FEMA, and the United States Coast Guard (USCG). To address the declassification of applicable records generated by the component agencies, USSS and FEMA have created declassification guides that identify program specific information that is exempt from automatic declassification and that have been

[1] 5 U.S.C. § 552a.

approved by the Interagency Security Classification Appeals Panel. In all other instances where an approved exemption from automatic declassification does not exist, DHS component generated classified information is automatically and properly declassified, or, where such records contain the equities of other agencies, referred to the appropriate agencies. As such, and pursuant to Executive Order 13526, DHS routinely reviews information to affirm classification and to declassify when possible. Most information currently declassified by DHS resides in Presidential Libraries and the National Archives and Records Administration, and is subject to external publication schedules.

Pursuant to Executive Order 13526, DHS instituted a fundamental and comprehensive review of all existing DHS security classification guides. The purpose of the review was to evaluate the guide content, assess the applicability of the guidance to the current operational environment, and ensure the guidance conformed to the standards for classification as cited in the Order. A summary of these efforts can be found on the Information Security Oversight Office's webpage: http://www.archives.gov/isoo/fcgr/index.html.

In 2013, the DHS Office of the Inspector General issued DHS-OIG 13-106, *Reducing Over-Classification of DHS' National Security Information*, which reviews the classification program at-large at DHS.

An overview of this report is at http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_SLP_13-106_Jul13.pdf, and the full report at http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-106_Jul13.pdf.

Emphasis on Plain Writing

DHS understands that plain writing is vital for achieving the goals of Open Government. According to the Plain Writing Act of 2010, plain writing is, "writing that is clear, concise, well-organized, and consistent with other best practices appropriate to the subject or field and intended audience. Such writing avoids jargon, redundancy, ambiguity, and obscurity." The Department has a plain writing implementation plan in place and is committed to improving communication in support of the Plain Writing Act of 2010.

To view the Plan Writing Implementation Plan, please visit http://www.dhs.gov/dhs-plan-implement-plain-writing-act-2010-requirements-summary.

If you have any questions or comments regarding plain language, please submit them here: http://www.dhs.gov/comment-dhsgov-website.

V. Participation and Collaboration

While there are many examples of successful partnerships across the homeland security enterprise, more work is needed to infuse the culture of partnerships across homeland security missions and issues. The public and private sectors share a strategic opportunity to look closely at new areas for partnership, scale up successful partnerships, and continue to advance a structured approach to partnering on homeland security challenges. The Department is developing a Public-Private Partnership Toolkit, to be released concurrently with the Quadrennial Homeland Security Review, to increase collaboration and participation.

The Public-Private Partnership Toolkit

DHS is keenly aware of the essential role it plays every day in facilitating the lawful trade of goods and services—trade that is vital to our economic security and competitiveness. The Department shares a vital core mission with the Department of Commerce (DOC). Security does not just support public safety, it also supports the economy. As a result, DHS will be partnering with the DOC to collaborate with the public and private sectors in the following areas:

> "I am pleased to present the following Public-Private Partnerships Toolkit, which furthers the important conversation about partnerships through the homeland security enterprise. Our relationship with the private sector is tremendously important, and we must highlight, foster, and encourage development of successful public-private partnerships."
> *– DHS Secretary, Jeh Johnson*

- **Security and trade are mutually reinforcing**
  Commerce and public safety are mutually reinforcing. Promoting the secure and legitimate flow of goods and people—and focusing our resources on preventing the illegal movement of people and goods that pose a potential threat to our citizens, businesses, and our way of life—is good for our economy and our security.

- **The private sector is a crucial partner in our shared goals of security and economic competitiveness**
  Government programs and policies that affect the private sector are more effective when designed in collaboration with affected stakeholders—and better executed when they appropriately tap market forces to encourage private investment in public goods.

- **The public deserves integrity and good service from its government**
  Competent, efficient, and responsive service must be a priority in all programs that involve direct interaction with the public. Good service facilitates compliance with laws and regulations, eases burdens on people and businesses, enhances the value provided to the Nation, and promotes trust in government.

The DHS Public-Private Partnerships Toolkit was developed as part of the 2014 Quadrennial Homeland Security Review Public-Private Partnerships Study and will be released concurrently with the Review. A Public-Private Partnership is a collaborative working relationship between DHS (and/or federal, state, local, tribal, and territorial government partners) and non-government actors, in which the goals, structure, roles and responsibilities of each partner, as well as decisions, as appropriate to the partnership, are mutually determined.

This toolkit provides a structured way of thinking about partnerships that focuses discussions on interest alignment, desired outcomes, and partnership models for homeland security. While this toolkit supports consideration of important issues related to partnerships, it is not meant to disrupt or interfere with existing partnerships.

Loaned Executive Program

The Loaned Executive Program was created in August of 2008 to provide private sector top executive-level and subject matter experts an opportunity to share their expertise with the U.S. Department of Homeland Security.

The program is a special opportunity that provides executive-level talent from the private sector an opportunity to share their expertise with Homeland Security to fill special, discrete needs. Through the program, the Department is working with the private sector on innovative solutions to our homeland security challenges. DHS is looking to the nation’s top executives and industry experts to partner with us as we strive to solve problems, improve processes, and fully realize our mission. Serving as a loaned executive provides an opportunity to make a meaningful difference by protecting our nation. Loaned executives serve a maximum of one year as an unpaid employee of the Department.

For additional information, please visit: http://www.dhs.gov/loaned-executive-program.