Open Government Plan 2.0

U.S. Department of Homeland Security

Homeland Security

Table of Contents

I. Introduction

In April 2010, the Department of Homeland Security (DHS) released Open Government Plan Version 1.0 which explored current activities that exhibit open government in DHS and charted a path for increasing transparency, collaboration and partnership in the Department. In June 2010, the Department published an updated version of the DHS plan to more fully address the Open Government Directive. Throughout the remainder of 2010, the Department engaged in ongoing efforts to expand and enhance the ways DHS encourages transparency, public participation and collaboration. Open Government Plan Version 2.0 outlines these efforts for the public. Such actions include:

- Hosting open dialogues to receive comments and ideas from the public on cybersecurity and National Preparedness using GSA's online collaboration tool IdeaScale;
- Providing an update of the Department's social media tools; and
- Providing additional datasets to data.gov.

As prescribed by President Obama, DHS and all Federal agencies are working to reduce their backlog of Freedom of Information Act requests. The Department's Chief Privacy Officer issued guidance to DHS components laying out an aggressive plan to reduce DHS FOIA backlog requests by 15 percent per year. The FOIA plan calls for monthly meetings and quarterly reviews to ensure the Department is successful in reducing its backlog. In addition, the Chief Privacy Officer has bolstered proactive disclosure by augmenting an earlier policy memo with a robust plan.

In addition to enhanced public participation opportunities, the Department has inventoried over 900 datasets of an estimated universe of 1200 and has developed a dataset candidate pipeline of over 70.

The following Open Government Plan highlights:

- How the principles of Open Government align with DHS missions
- The DHS governance structure for managing Open Government
- Data.gov activities
- Performance management for key Open Government activities
- Existing and new flagship initiatives

II. DHS Missions and Open Government

DHS Mission Area 1: Preventing Terrorism and Enhancing Security

The Department was created to improve coordination, reduce redundancies and facilitate the exchange of information to help protect the nation from threats of all kinds.

The Department's vision is a secure and resilient Nation that effectively prevents terrorism in ways that preserve freedom and prosperity. To achieve success in this mission area the Department has established collaborative agreements, partnerships and cooperation with federal agencies, across levels of government, and between the government and private institutions.

Collaboration is an important element of preventing terrorism and enhancing security. Over the past year, the Department led an unprecedented effort to increase international and domestic aviation security measures. Fusion Centers remain the centerpiece of state, local, and federal intelligence-sharing for the future, gathering information at the local level to analyze that information and convert what might be seemingly isolated bits of data into actionable intelligence. This compilation of data works to identify patterns and trends at a state or local level, illustrating potentially greater threats.

Additionally, the July 2010, DHS-wide Blue Campaign to combat human trafficking through enhanced public awareness, victim assistance programs, and law enforcement training and initiatives is guided by collaboration. For more information, visit: www.dhs.gov/humantrafficking.

The "If You See Something, Say Something" campaign—originally implemented by New York City's Metropolitan Transit Authority and funded, in part, by $13 million from DHS' Transit Security Grant Program—intends to raise public awareness of indicators of terrorism, crime and other threats and emphasize the importance of reporting suspicious activity to the proper transportation and law enforcement authorities.

The "If You See Something, Say Something" campaign complements the Nationwide Suspicious Activities Reporting (SAR) Initiative (NSI) —a partnership among federal, state, and local law enforcement to establish a standard process for law enforcement to identify and report suspicious incidents or activity and share that information nationally so it can be analyzed to identify broader trends.

The NSI is a new national information-sharing partnership with Amtrak in which DHS and the Department of Justice work with Amtrak to employ the latest tactics and strategies in law enforcement trainings on how to identify suspicious behaviors associated with new and evolving threats. Amtrak officers will also use an upgraded reporting system—made available by the Transportation Security Administration—to refer suspicious activity reports to DHS and the Federal Bureau of Investigation for analysis and follow-up.

In July 2010, Secretary Napolitano highlighted the partnerships that support state and local law enforcement and community groups across the country, including the Homeland Security Advisory Council's (HSAC) (http://www.dhs.gov/files/committees/editorial_0331.shtm)"Countering Violent

Extremism" Working Group—comprised of chiefs of police, sheriffs, community leaders and homeland security experts. Following a February tasking from Secretary Napolitano, the working group provided recommendations (http://www.dhs.gov/xlibrary/assets/hsac_cve_working_group_recommendations.pdf) on ways DHS can better support community-based efforts to combat violent extremism in the United States. The first sets of concrete next steps for supporting community-based efforts to address homeland security threats are available at (http://www.dhs.gov/xlibrary/assets/fact_sheet_reduce_violent_crime_080310.pdf).

Since 2005, the United States Coast Guard (USCG) has operated the America's Waterway Watch (AWW) program. The original AWW is a combined Maritime Domain Awareness (MDA) effort of the active duty USCG and its Reserve and Auxiliary components. The program serves to educate citizens about threats, enlists the active participation of those who live, work or play around America's waterfront areas, and provides a means for reporting suspicious activity to responsible authorities.

More recently, the USCG has formalized the structure for the America's Waterway Watch 2.0 (AWW 2.0) program. AWW 2.0 is an enhancement of the original AWW program that allows for a unified national program encompassing local all-hazards MDA operations. It leverages public and private resources to protect the maritime economy and the environment, defends our maritime borders, and assists those persons in peril in the near shore environment. AWW 2.0 improves MDA and provides an overarching mechanism to improve maritime security and enhanced USCG response and prevention capacities by integrating elements of an award winning, local USCG program called the Citizen's Action Network (CAN).

CAN is a civilian volunteer-based maritime domain collaboration group that readily interacts with the local USCG sectors in support of search and rescue, marine environmental response, law enforcement, port security and other essential mission areas. Active duty, reserve and auxiliary members at the district and sector level recruit citizens in the port and coastal maritime communities to volunteer their time and vantage point as additional asset when requested.

In August 2010, TSA took another step forward in strengthening the security of air travel, meeting a key requirement of the 9/11 Act by screening 100 percent of air cargo on domestic passenger aircraft. TSA worked closely with the cargo and aviation industries to fulfill the Congressional mandate by the Aug. 1, 2010 deadline (http://www.tsa.gov/press/releases/2010/0802.shtm).

To meet the domestic mandate, TSA created the Certified Cargo Screening Program (CCSP) (http://www.tsa.gov/what_we_do/layers/aircargo/certified_screening.shtm), which allows certified facilities across the country to screen cargo before it reaches the airport.

Prior to the August 1, 2010 deadline, more than 900 facilities became CCSP certified. This innovative program spreads the cargo screening responsibility, on a voluntary basis, across the supply chain to manufacturing facilities and distribution centers.

DHS Mission Area 2: Securing and Managing Our Borders

A safe and secure homeland requires that the Department maintain effective control of air, land, and sea borders to prevent illegal trafficking that threatens the United States, while facilitating lawful travel and trade.

Succeeding in this mission area requires resources, collaboration and stakeholder engagement. The Department's U.S. Customs and Border Protection (CBP), U.S Immigration and Customs Enforcement (ICE), and the U.S. Coast Guard work closely with stakeholders and law enforcement officials to manage the flow of legal and illegal persons and contraband across U.S. borders and ports of entry.

The best examples of collaboration in securing and managing the borders are the Border Enforcement Security Taskforces (BESTs), which ICE leads. BEST is an innovative model for collaborative law enforcement. To date there are 12 BESTs, eight of which are on the southwest border, and include the participation of ICE, CBP, the USCG, and the DHS office of Intelligence and Analysis (I&A) on the DHS level; the Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the Federal Bureau of Investigation (FBI), and U.S. Attorney's offices. Mexican law enforcement agencies also participate in BEST, and the government of Mexico has agreed to provide representatives to every BEST team on the southwest border.

To collaborate with and engage the public, the Department uses *"Our Border"* (http://ourborder.ning.com/), an open online collaborative platform that allows the public to connect and communicate with officials at the Department of Homeland Security who are working together to address border issues. Through *Our Border*, the Department:

- Educates stakeholders about its policies and programs;
- Empowers stakeholders to contribute in the decision process that affect their lives and businesses;
- Listens to stakeholders to better understand and meet their needs;
- Engages stakeholders in collaborative problem solving;
- Facilitates the sharing of best practices among stakeholders; and
- Expands the network based on stakeholders geography, industry, port of entry, and mutual interests.

DHS Mission Area 3: Enforcing and Administering Our Immigration Laws

The Department enforces the Nation's immigration laws while streamlining and facilitating the legal immigration process (http://www.dhs.gov/files/immigration.shtm). To assist with the enforcement and administration of the Nations immigration laws the Department's U.S Citizenship and Immigration Services (USCIS) has a website to communicate information on immigration services, procedures and forms needed to make the process more transparent and user friendly for the public. The USCIS website (http://www.uscis.gov/portal/site/uscis)-- available in both English and Spanish - provides information needed to better understand immigration services and policies. Recent

enhancements to the website include: real-time alerts on the status of immigration applications via text message and email, meeting announcements and RSVP instructions, background materials, meeting summaries and questions and answers from previous meetings.

In early September 2010, ICE Director, John Morton, made an historic trip to Asia to build international investigative cooperation, especially with regard to intellectual property rights (IPR) enforcement between ICE and law enforcement authorities in China and South Korea.

Some of the most pressing investigative issues under ICE's jurisdiction include intellectual property rights enforcement, counter-proliferation, cyber crime, money laundering and human trafficking and smuggling.

In April 2010, ICE launched the Online Detainee Locator System (ODLS), a public, web-based tool designed to assist family members, attorneys and other interested parties in locating detained aliens in ICE custody. The creation and implementation of the ODLS is a concrete example of the Department's commitment to transparency and detention reform.

The ODLS is located on ICE's public website, http://www.ice.gov, and provides the public with information on the location of the detention facility where a particular individual is being held, a phone number to the facility and contact information for the ICE Enforcement and Removal Operations office in the region where the facility is located. A brochure explaining how to use the ODLS is available on the website in: English, Spanish, French, Mandarin, Vietnamese, Portuguese, Russian, Arabic and Somali.

"The ODLS is an easy, accessible tool that allows family members and counsel to locate an individual in ICE custody in a matter of minutes," said Phyllis Coven, acting director of ICE's Office of Detention Policy and Planning. "ICE is making great strides in our effort to translate the principles of reform into innovative, practical and timely solutions."

To learn more about ICE's detention reform, please visit: http://www.ice.gov/dro/detention-reform/. An ODLS brochure is available at following URL: http://www.ice.gov/news/library/factsheets/odls.htm

DHS Mission Area 4: Safeguarding and Securing Cyberspace

Cybersecurity is one of the most pressing issues of our time.

To safeguard and secure cyberspace, the Department is working to strengthen existing

"People cannot value security without first understanding how much is at risk. Therefore, the Federal government should initiate a national public awareness and education campaign…This campaign should focus on public messages to promote responsible use of the Internet and awareness of fraud, identity theft, cyber predators, and cyber ethics."—President Obama, Cyberspace Policy Review June 2009

partnerships with the private sector to help secure the networks that power the economy and the internet domain; and is striving to educate the public on the shared responsibility of cybersecurity.

Partnerships with the private sector help the Department improve coordination among the government, private sector and international governments. Current partnerships include: the National Cyber Security Division, U.S. Computer Emergency Readiness Team, (US-CERT); and the National Cyber Security Center. Through US-CERT and other programs, the Department is working more closely than ever with the private sector to detect and understand threats, share knowledge, and learn from the best that the private sector has to offer. Secretary Napolitano stated that she believes this kind of partnership with the private sector can provide a model for deeper engagement to protect our nation's critical infrastructure. USCERT alerts http://www.us-cert.gov/current/

In addition to working with the private sector to develop strategies and solutions to safeguard and secure cyberspace, the Department also leads the development and execution of the National Cybersecurity Campaign. The Campaign is one of the Department's flagship initiatives for Open Government 2.0; is aimed at raising awareness about cybersecurity, increasing the public's understanding of cyber threats, and empowering them to be prepared and cyberspace secure.

The Department kicked off its Cybersecurity Awareness Campaign Challenge (http://www.dhs.gov/files/cyber-awareness-campaign.shtm), in conjunction with National Cybersecurity Awareness Month. The winners of the challenge partnered with the Department as part of the planning of the National Cyber Security Awareness Campaign.

DHS Mission Area 5: Ensuring Resilience to Disasters

The Department's role in ensuring resilience to disasters is grounded in the four traditional elements of emergency management: hazard mitigation, increasing preparedness, effective emergency response, and supporting community recovery. During domestic incidents, the Department's role, largely executed through the Federal Emergency Management Agency (FEMA), is principally one of coordinator, working closely with State, local, tribal, and territorial partners to enhance preparedness, build and sustain capabilities, and act as an aggregator of resources from across the Federal government. DHS maintains a significant first responder capability for disasters in the maritime domain through the U.S. Coast Guard (USCG), and also ensures the resilience of critical infrastructure to disasters through the National Protection and Programs Directorate. DHS, through FEMA, also has specific direct responsibilities, including disaster response and field coordination, disaster logistics, individual and public assistance programs, as well as national continuity programs. In those instances, however, DHS's primary role is to support the efforts and priorities of local communities as they prepare to prevent, protect against, respond to and recover from an incident.

Restore the Gulf of Mexico/ Deepwater Horizon Oil Spill Response

The Department played a lead role in the federal response efforts to the Deepwater Horizon oil rig explosion in the Gulf of Mexico. DHS deployed the USCG to search and rescue the 126 people working on the oil rig, and quickly lead efforts to establish a command center on the Gulf Coast to

address the potential environmental impact of the event; and coordinated with all state and local governments. Secretary Napolitano led the National Response Team, an organization of 16 federal departments and agencies responsible for coordinating emergency preparedness and response to oil and hazardous substance pollution events.

The USCG played a major role in the response effort from the very beginning, when it responded to the explosion on a search and rescue mission. The federal on-scene coordinator led a regional response team that included DHS, Department of Commerce/National Oceanic and Atmospheric Administration, Department of Interior and the Environmental Protection Agency, as well as state and local representatives. As the event escalated, U.S. Coast Guard Admiral Thad Allen was announced as the national incident commander for the administration's continued, coordinated response—providing additional coordinated oversight in leveraging every available resource to respond to the Deepwater Horizon oil spill and minimize the associated environmental risks.

The Department along with other federal agencies created the RestoretheGulf.gov as the official federal portal for the Deepwater Horizon oil spill response and recovery. The site provides the public with information on the response, current operations, news and updates, instructions on how to file a claim and obtain other assistance, and links to federal, state and local partners.

Office of Intergovernmental Affairs and FEMA Host National Dialogue

In April 2010, Secretary Napolitano convened the Local, State, Tribal, and Federal Preparedness Task Force (http://www.fema.gov/preparednesstaskforce/index.shtm) to assess the state of national disaster preparedness and make recommendations for improvement. Since April, the Task Force has participated in face-to-face meetings, teleconferences, and web-based collaborative efforts to supplement and build upon the discussions of the Task Force membership. In September 2010, FEMA hosted leaders from the emergency management and disability communities to discuss strategies to integrate the entire community into planning for emergencies

The second phase of the Task Force's objectives includes engaging the public to help the Department identify similarities and differences in how various organizations view preparedness issues.

The Department's Office of Intergovernmental Affairs, FEMA, and the National Protection and Programs Preparedness Directorate hosted a national dialogue to hear directly from individuals across the country about the importance of preparedness (http://preparedness.ideascale.com). The dialogue closed on August 31.

III. Open Government Governance

The Department established a governance structure consisting of senior executives and managers to form various working groups within the Department to institutionalize Open Government at DHS. Figure-1 illustrates the governance structure within DHS and the functions of the working groups are described in the remainder of this section.

DHS convened an executive steering committee to evaluate the three pillars of the Open Government Directive in accordance with the Department's mission. The executive steering committee serves to adjudicate issues that cannot be resolved at the working group levels and sets policy decisions that are carried out by the working groups. The working groups engage in cross component outreach to disseminate direction received from the Executive Steering committee and engage in interagency collaboration efforts for a consistent Open Government focus.

At the direction of the Deputy 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 to the working groups utilized to oversee Open Government, the offices identified below continue to 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.

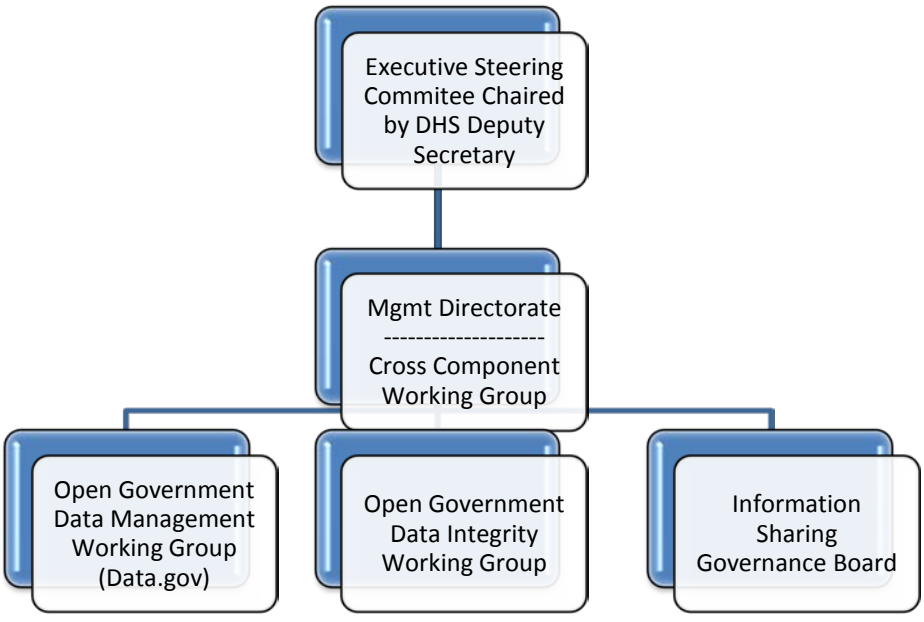


Figure 1. Governance Structure.

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 (OGD) and ensure that the Open Government Plan reflects the operations of the Department. This group meets monthly to discuss progress, roadblocks and new ideas for the Department's continued evolution of the three pillars as well as receive updates from representatives from the Data Management Working Group and the Data Integrity Working Group.

Data Management Working Group

The Office of the Chief Information Officer (OCIO) utilized its cross-component Data Management Working Group (DMWG) to identify three datasets required by the OGD for posting by the deadline prescribed. The DMWG defines, promotes and monitors enterprise data management practices across the Department. OCIO is leveraging the DMWG and the Data Asset Catalog to identify, prioritize and review the quality of new datasets moving forward.

Data Integrity Working Group / Senior Management Council

The DHS Under Secretary for Management (USM) is leading the critical activities required to implement the Office of Management and Budget's (OMB) Open Government Directive (OGD). The DHS Chief Financial Officer (CFO) has been designated Senior Accountable Official (SAO) for Data Quality under this Directive and will be 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 will provide 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 USM has requested Components designate their own SAO to work with the DHS SAO 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 (SMC) will provide 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. Once again, DHS is leveraging existent, effective infrastructure to accomplish key objectives.

Information Sharing Governance Board (ISGB)

The Information Sharing Governance Board (ISGB) is composed of executive leaders from the Components and offices 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 ISGB arbitrates inter-component information access delays and

denials, leads strategy in DHS information-sharing and collaboration activities, and ensures that the Department speaks with “one voice” to its external partners.

Offices

Privacy Office

In order to support the OGD, the Privacy Office has taken the lead on providing guidance for proactive disclosure of information. The Privacy Office continues to maintain 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 additional electronic reading rooms within DHS operational components, and a significant reduction in backlogged FOIA requests.

Office of the Chief Financial Officer

The Chief Financial Officer (CFO) serves as the Senior Accountable Official for the DHS Data Quality Plan for Federal Spending Information in support of the OGD. Currently the CFO is evaluating existing financial working groups, and possible modifications of those working groups, to form a well-rounded governance body and framework to ensure the quality of federal spending information. The CFO continues to provide 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, Web Management, and Employee Communications. All of these offices work in tandem to support comprehensive information flow to the public, media and employees. The Office of Public Affairs continues to maintain the Open Government web page on 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 build 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

DHS created the Private Sector Office to build relationships with the private sector and interface with other relevant Federal agencies on issues related to industry. The Private Sector Office continues to engage businesses, trade associations and other non-governmental organizations to foster dialogue with the Department. A key component to outreach efforts is managing stakeholder groups and keeping them informed on DHS policies that could impact them to promote public-private partnerships and best practices.

Office of Legislative Affairs

The Department values communications with Congress as central tenant of its open government efforts. The Office of Legislative Affairs (OLA) 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.

IV. Enhancing Data.gov

Area of focus: Data Asset Catalog

The purpose of the Data Asset Catalog is to store information about the Data Assets used to accomplish the mission of homeland security. Each DHS Component is responsible for maintaining an accurate, up to date description of its data assets within the Data Asset Catalog under DHS policy, and as documented in the Enterprise Data Management Concept of Operations. Progress on this initiative has been captured for the past three years on the Enterprise Data Management Scorecard, which is presented quarterly to the DHS CIO Council.

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, 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 Emergency Support Module.

The DHS Data Asset Catalog currently includes approximately 900 data assets of an overall total of 1,200 data assets. The majority of the remaining 300 data assets will be included in the catalog in Fiscal Year 2011 through continued support of the Data Management Working Group.

The information in the Data Asset Catalog 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 our private sector partners. Because of its homeland security and national security missions, the categorization of the Data Asset Catalog shows that only 5 percent of the 900 data assets contain data that is releasable to the general public.

One of the primary purposes for the collection of the data asset catalog is in support of the Department's information sharing mission, as a method for ensuring broad understanding of DHS data assets. The Data Asset Catalog is used to allow discovery of the data across 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 the data asset catalog 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 will be added to the Enterprise Data Management Scorecard in the 2011 timeframe. In this process, the data owners will 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 will be put through the Department's Open Government Initiative review process to address legal, financial, privacy and security concerns with release ability, which will result in the publishing of publically releasable data. Of the 900 data assets, approximately one third have been reviewed, resulting in a list of 75 candidate datasets in the process of review.

Challenges/Solutions

Challenges

A challenge the Department faces in registering datasets with Data.gov is that many of the Components do not have readily available server space that is accessible from outside of DHS. The Department has secured some space through the DHS internet server to provide hosting space for these datasets. The amount of space available is limited, and the Department continues to pursue other potential hosting solutions. The Data.gov Program Management Officer (PMO) intends to provide hosting space for datasets. DHS will consider this option as the service details become known.

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 strike a delicate balance between the need to safeguard and the responsibility to disclose information to the public. The Department has established a collaborative

review process to ensure that the data provided informs the public without compromising security. This review process currently takes an average of one month 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 and due to the "For Official Use Only" (FOUO) classification. Many of these datasets are suggestions received from the general public.

Below are a few examples:

Dataset	**Component**	**Rejection Reason**
LandScan USA	NPPD	Contains FOUO data essential to the value of the dataset
HSIP Freedom Geo-layers (160+)	NPPD	Contains FOUO data essential to the value of the dataset
Location and time of illegal border crossings and drug seizures	CBP	Contains FOUO data essential to the value of the dataset
FOIA Claims http://www.tsa.gov/assets/xls/claims_07152008.xls	TSA	The file linked is not FOIA Claims but damaged baggage claims, which duplicates another public suggestion
Racial profiling in airports to prevent terrorism	TSA	TSA does not engage in racial profiling
Immigration Subset = Legal | Illegal	USCIS	Request is not specific to USCIS – too broad in scope
Immigration, laws, policies enforcement, changes in the last 50 years	USCIS	Request is not specific to USCIS – too broad in scope

Dataset	Component	Rejection Reason
Immigration statistics and how that relates to the population of Hispanics in the U.S. How many Mexican-Americans move back and forth between the two countries? Or how many baby boomers are retiring in Mexico?	USCIS	USCIS does not track foreign residences of U.S. citizens.
It will be great if USCIS post current backlog for Highly skilled immigrants waiting for green card based on their Priority date	USCIS	Data is accessible through Department of State
Emigration	USCIS	Request is not specific to USCIS – too broad in scope
Every month DOS/USCIS publishes Visa Bulletin, which describes who are eligible to get Green Card, but then they don't mention how many visas are used or are available for the current fiscal year instead the mighty word used is "DUE to HIGH LOAD". It would be great to have that data available so for the folks waiting for visa availability, this data might give more transparency as to what DOS/USCIS is doing.	USCIS	Data is accessible through Department of State
Merchant and Recreational Vessels	USCG	Deemed Inappropriate by Privacy Office
Port State Information Exchange (PSIX)	USCG	Deemed Inappropriate by Privacy Office

Solution

In order for Data.gov to be successful, the process must work with Components offices. Training materials in development will help educate program owners about Data.gov, and will be required for all program managers. Governance structure requires a Data.gov lead at each Component. DHS must successfully transition the pipeline and submission process responsibility to each Component in FY2011 in order to grow Data.gov participation.

Data.gov and:

Accountability

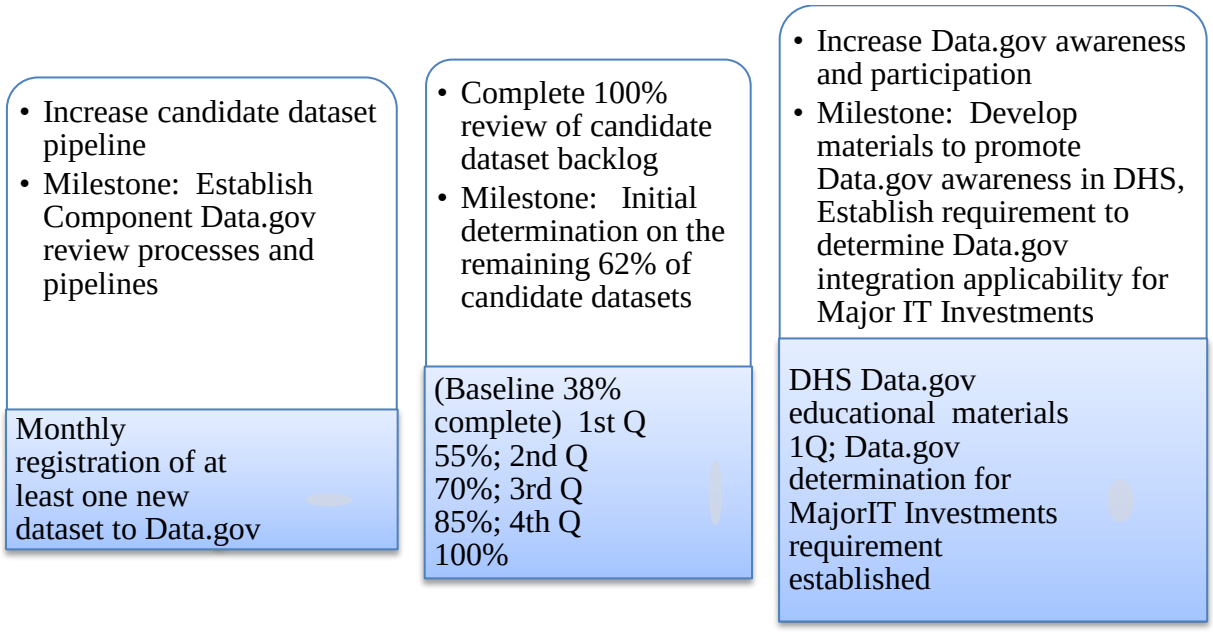


Figure 2 – Accountability Metric

Candidate datasets are identified in a number of ways. First, the Deputy Secretary's executive steering group 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 and programs self-nominated datasets they could contribute. Suggestions have also been received from the Data Management Working Group. OCIO identified data that is already published by the Department through component websites, which can be provided in a more open, usable format. OCIO has established a site on the DHS intranet where DHS employees can view the 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 PMO. When suggestions for information are 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?

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 candidate dataset pipeline is tracked by component. The pipeline summary (Figure-3) is provided to the DHS OCIO Council to keep component information officers apprised of issues. The detailed pipeline of specific candidate datasets is provided in Appendix B.

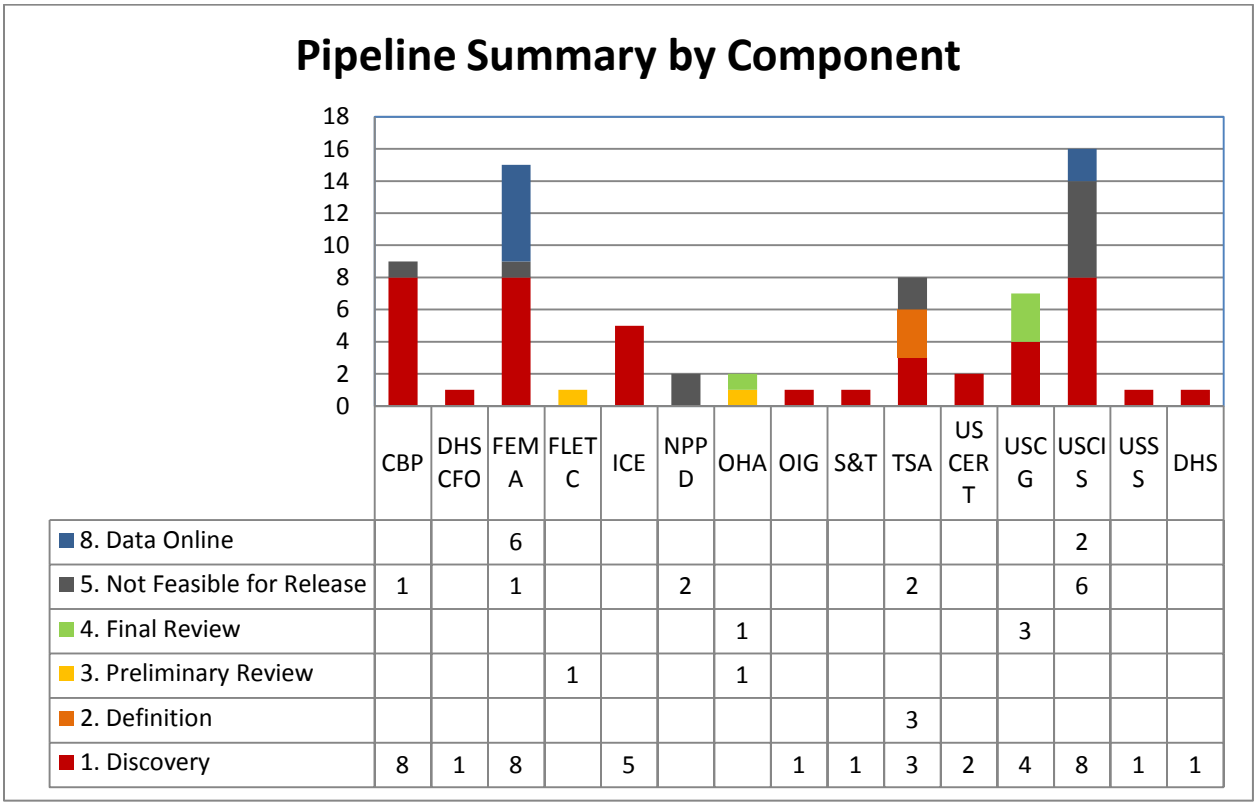


Figure-3 - Data.gov Pipeline Summary by Component

DHS OCIO will develop and provide training materials to promote awareness of Data.gov across the Department programs. The training will provide 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.

DHS OCIO is investigating the ways in which Data.gov integration can be tied to existing oversight processes. One potential method is to include data dissemination determinations into the Systems Engineering Life Cycle (SELC). Each project producing a data structure would be asked to consider the widest allowable audience for data dissemination, including releasing the data to the general public through Data.gov.

Another oversight method that can be leveraged is the Office of Management and Budget (OMB) Exhibit 53/300; summary of budget estimates for all Information Technology investments. Per the OMB process, each agency submitting an Exhibit 53 must answers questions indicating whether or not the their IT investment is providing data to Data.gov. DHS can potentially leverage this process to identify Data.gov candidates or to provide the reason why a particular investment should be excluded from participation.

Institutionalizing Data.gov

OCIO is working to institutionalize 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 will incorporate 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. DHS is working to promote a culture of information sharing, and that all data should be considered for release to:

- the general public;
- state, local, tribal, and commercial partners;
- other Federal agencies through the PM ISE; and
- other DHS Components and programs.

OCIO has developed materials to educate DHS employees about the Open Government initiative and Data.gov to promote awareness and participation. This training will be available to all DHS program managers in FY 2011.

DHS OCIO is also working with the Components, the Data Management Working Group, 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. USCIS has also established a Data.gov lead and is working to incorporate Data.gov processes into their data environment. The Department is committed to providing the public with high value data while safeguarding sensitive information necessary to meet the mission of DHS.

V. Measuring progress

Since the release of the Open Government Directive, DHS has taken a number of steps to promote transparency in its mission. The Department released its Quadrennial Homeland Security Review of the Department's strategic framework and offers a vision for a secure homeland, specifies key mission priorities, and outlines goals for each of those mission areas. It also created a Data Management working group to review the Department's data inventory and identify what datasets can be released to the public and posted on data.gov. In addition, the Department is also developing a plan to help institutionalize proactive disclosure and the Freedom of Information Request process (FOIA).

a) **FOIA backlog reduction**- The Department set a goal to reduce its backlog request by 15 percent annually. Despite a nearly 30 percent spike in incoming requests in FY 2010, the Department surpassed its goal by reducing the overall FOIA backlog by 40 percent.
b) **Proactive disclosure-** Since August 2009, the Department has released/posted approximately 700 documents to its FOIA reading rooms. The Department is developing a plan to institutionalize proactive disclosure across DHS by the end of FY 2011.

Freedom of Information Act

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.

Following the creation of the Department, the complex mission of the agency prompted many inquiries and FOIA requests. While generating many inquiries because of its new status and mission, DHS also began its operations with an inherited FOIA backlog by virtue of the fact that several significant existing agencies were merged into DHS: the U.S. Coast Guard, Secret Service, United States Customs Service, Immigration and Naturalization Service, Federal Emergency Management Agency, Transportation Security Administration, Federal Protective Service, and the Federal Law Enforcement Training Center. At the time of the merger of these agencies into DHS, each maintained FOIA backlogs, with one component's backlog measured at 25,515.

As of September 15, 2006, the DHS-wide backlog was 98,103. Over the past four years, DHS decreased its FOIA backlog by 81 percent and the FY 2009 *DHS Annual FOIA Report* (http://www.dhs.gov/xlibrary/assets/foia/privacy_rpt_foia_2010.pdf) documents 18,918 backlogged requests Department-wide. In order to reduce the FOIA request backlog at DHS by a minimum of 15 percent each year, each component receives a monthly goal, setting the number of requests that must be processed in that month. The goals, individually tailored to each component, use the average

number of requests received per month and the upper limits of the component's processing capacity. Meeting these goals keeps the Department on track to reduce the FOIA backlog in accordance with the Directive (http://www.justice.gov/ag/foia-memo-march2009.pdf). The Chief FOIA Officer continually reviews the progress made in the reduction of the backlog and the components' capacity to keep up with the incoming requests. As a result of this ongoing review, the Chief FOIA Officer is able to work with components to assist in removing any impediments that interfere with efficient FOIA request processing.

The Chief FOIA Officer also holds bi-weekly conference calls with the component FOIA officers to discuss FOIA policy and processes. These meetings allow the Chief to stay abreast of any concerns or problems related to the administration of FOIA, provide clarity and guidance related to new developments in FOIA, such as, proactive disclosure and the Open Government initiative, and also allows component FOIA officers to share best practices.

As part of the DHS FOIA Office's commitment to transparency, the Office works with the National Archives Office of Government Information Services (OGIS) as appropriate. The OGIS resolves federal FOIA disputes by providing mediation services between FOIA requesters and federal agencies, reviews policies and procedures of administrative agencies under FOIA, reviews agency compliance with FOIA, and recommends FOIA policy changes to Congress and the President. Further, the Department is in the final stages of updating its FOIA Regulations. The regulations are currently in final draft form, and the Notice of Proposed Rulemaking (NPRM) should be released in the Unified Agenda of Federal Regulatory and Deregulatory Actions by early in 2011.

The DHS FOIA backlog reduction plan can be found here:
(http://www.dhs.gov/xlibrary/assets/foia/privacy_foia_backlog_reduction_goals_table_11-30-07.pdf)

Proactive disclosure

The Freedom of Information Act outlines the transparency requirements government agencies must follow. Subsection (a)(2) requires each agency to make four distinct categories of records affirmatively available for "public inspection and copying."

On August 26, 2009, DHS Chief Privacy Officer Mary Ellen Callahan issued the *Proactive Disclosure Memorandum* to inform the proactive disclosure process. In that memo, Ms. Callahan directed the Department to include the following categories of records on their agency websites and link them to their respective electronic reading rooms:

- 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 & grants;
- Management Directives and instructions;
- Congressional correspondence under DHS control;
- FOIA logs; and

- Any records released pursuant to a FOIA request that have been, or are likely to become, the subject of three or more requests.

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*.

The Department's Proactive Disclosure Initiative has been extremely successful. Approximately 700 documents have been proactively disclosed, and the Department plans to regularly disclose more documents in the future. For example, CBP has posted more than 80 documents, including Congressional correspondence, contracts, final opinions, FOIA logs, manuals and instructions, and significant records of interest. FLETC posted its strategic plan, organizational structure, financial reports, and training materials that are not considered law enforcement sensitive, and the Privacy Office posted Volumes 8000-11000 of Departmental directives as well as the FOIA logs for FY 2004-2009.

In light of the continued increase of proactively disclosed documents in the DHS FOIA Electronic Reading Room (http://www.dhs.gov/xfoia/editorial_0424.shtm), the FOIA Office has worked diligently to enhance its FOIA Electronic Reading Room to better accommodate its robust collection of documents. The Electronic Reading Room is linked on the front page of the DHS Privacy Office website, categorized by document type, and includes a "Frequently Requested" document section.

Declassification of Department of Homeland Security Information

Only in existence since 2003, the Department of Homeland Security (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 Federal Emergency Management Agency (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 approved by the Interagency Security Classification Appeals Panel (ISCAP). In all other instances where an approved exemption from automatic declassification does not exist, DHS component generated classified information is automatically 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 (NARA), and is subject to external publication schedules.

Pursuant to Executive Order 13526, DHS has instituted a fundamental and comprehensive review of all existing DHS security classification guides. The purpose of the review is to evaluate the guide content, assess the applicability of the guidance to the current operational environment, and ensure

the guidance conforms to the standards for classification as cited in the Order. Under this effort, each security classification guide published within DHS will be revised and reissued no later than June 2012.

National Declassification Center (NDC)

Created by Executive Order 13526, the "National Declassification Center" (NDC) was developed to streamline declassification processes, facilitate quality assurance measures, and implement standardized training across the executive branch relative to the declassification of records of permanent historical value. Since the bulk of all DHS historical records reside at the NARA facility in College Park, MD, DHS was an early and strong proponent of the NDC and looked upon it as a positive means to improve the process for the declassification of records containing multiple agency equities as well as a means to expedite public access to declassified records. DHS, along with experts from across the Federal government, continue to provide valuable processing input and expertise to the NARA in an effort to modernize the overall declassification system and make the NDC a success. More information regarding the National Declassification Center can be found online at http://www.archives.gov/declassification

Status of DHS Declassification Efforts

Of the estimated 400 million pages of records currently held at the NARA College Park Facility, only a small percentage (approximately 400,000 pages) fall under the purview of DHS, most of which have already been reviewed for declassification.

Department of Homeland Security Pages Reviewed and Declassified

	Reviewed	Declassified
FY2009	2,723	767
FY2008	18,765	3,864
FY2007	22,948	10,208
FY2006	239,470	3,626
FY2005	10,661	9,583
FY2004	10,007	9,681

Note: Does not include Mandatory Declassification Review (MDR) program

Source: National Archives and Records Administration *Annual Report to the President*

Presidential Libraries:

Documents residing at the Presidential Libraries are routinely scanned into the Remote Archives Capture (RAC) program for review by all executive branch agencies and the Department of Defense. Since the inception of the RAC Program, DHS has been aggressively reviewing these documents for possible release, exemption, exclusion or additional referrals. Documents scanned into the RAC program are processed and ready for public viewing in approximately six months.

Mandatory Declassification Review Requests (MDR):

The DHS process for submitting a mandatory declassification review request under the provisions of Executive Order 13526 are publically available and published in 6 C.F.R. Part 7, DHS Classified National Security Information. MDR's received from the public are processed through the DHS Departmental Disclosure Officer, Privacy Office. Referral requests received from other government agencies or via the Presidential Libraries are processed by the DHS Office of the Chief Security Officer/Administrative Security Division. Since 2004, the Department of Homeland Security has reviewed over 1068 MDR's, comprising of over 52,600 pages. Of those pages reviewed, approximately 40,021 pages were declassified either in full or in part.

FOIA Requests:

The Privacy Office is responsible for administering policies, programs, and procedures to ensure that Department of Homeland Security complies with the Freedom of Information Act (FOIA) and the Privacy Act of 1974, 5 U.S.C. 552 and 5 U.S.C. 552a, respectively.

FOIA requires agencies to make various types of records available for public inspection in both paper and electronic form. These records are available for public viewing online in the DHS/FOIA Electronic Reading Room. Information regarding FOIA requests, frequently asked questions, contacts, statutes and resources can be accessed at http://www.dhs.gov/foia.

Data Integrity

The Department's CFO will assess the data provided by each Component to determine the quality of controls over the accuracy, completeness and timeliness of each submission. Components that award financial assistance will be required to certify data posted to USASpending.gov. In addition, DHS CFO will improve the accuracy and timeliness of data posted on USASpending.gov by promulgating best practices and implementing action plans.

Accountable Office – DHS CFO
Performance Metric (1): Increase and review the inventory of identified CFDA programs for submitting compliant data to USASpending.gov.
Milestones: Engage the CFO Council to review CFDA inventory and corresponding feeder systems of record by the end of FY 2011.
Anticipated Deliverable: 1Q 25 percentage; 2Q 50 percent; 3Q 75 percent; 4Q 100 percent inventory review. A report will be available 30 days after the end of each quarter.

Performance Metric (2): Increase the percentage of dollars posted to USASpending.gov with a Treasury Appropriation Symbol (TAS) throughout FY 2011.
Milestones: Achieve 25 percent of dollars posted to USASpending.gov in Q1; Q2 50 percent; Q3 75 percent; Q4 100 percent.
Anticipated Deliverable: Post quarterly report on the actual percentage achieved on the CFO's website. Report will be available 30 days after the end of each quarter.

Note: USASpending.gov data includes award amounts for contracts, grants, loans, and other assistance.

Figure 4 – Data Integrity Performance Metrics

DHS CFO will be unable to validate data or to ensure accuracy, completeness or timeliness of data until standardized and streamlined financial assistance business models, processes and supporting information technologies are implemented across the Department.

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 Assistant Reporting Working Group to discuss emerging issues	Recurring
Document current reporting process	October 2010
Identify a Financial Reporting Accountable Official for each Component	October 2010
Document way forward for USASpending.gov reporting	March 2011
Develop standard model for reporting	June 2011
Bring DHS closer to compliance with FFATA requirements.	August 2011

Milestones to support the accuracy, completeness and timeliness of all financial assistance data posted to any public venue	**Finish Date**
Train Financial Reporting Accountable Officials to ensure future FFATA compliance	August 2011
Develop business models and business rules related to reporting for the DHS-wide enterprise system.	December 2011

Table 1 – Data Integrity Milestones

Participation and Collaboration

The Department engages the public using social networking tools, public dialogues and web challenges to help the Department learn how we can better meet the interests of the public. If transparency is accountability and being open with the public; then participation is requesting information from the public to help improve its communications with the public. To cultivate this thinking, the Department engaged the public using GSA's IdeaScale for the QHSR and for the initial National Dialogue on Open Government and received over 300 comments. The Department is also engaging the public through its Cybersecurity Awareness challenge and via public outreach effort from the Homeland Security Advisory Council.

Outreach

One of the DHS advisory committees is the Homeland Security Advisory Council (HSAC). The HSAC is an organizationally independent advisory board of highly-distinguished leaders from state, local, and tribal government; first responder communities; the private sector; and academia who provide recommendations and strategic guidance to the Secretary. The Council announces all upcoming public meetings via the Federal Register Notice in accordance with the Federal Advisory Committee Act. In the Federal Register Notice, the HSAC encourages feedback its public email address. In addition, at each in person public meeting, our Council leadership again encourages public feedback to our email address hsac@dhs.gov.

The Department balances efforts to address evolving threats with complex responsibilities of prevention, response and recovery. By recognizing the shared goals of Federal, State, local, Tribal, nongovernmental, and private-sector partners, the Department engages with a wide array of external stakeholders to promote homeland security.

HSAC recently requested public comments regarding the Homeland Security Advisory System. These comments were passed to the Homeland Security Advisory Council's Homeland Security Advisory System Task Force. The Council received approximately 140 comments and a summary of these comments are posted on the HSAC website.

In order to increase public awareness of the Department's advisory committees, the Committee Management Office is in the process of improving its intranet page to provide more guidance on when interactions with non-Federal individuals or entities are covered under the Federal Advisory Committee Act (FACA).

On August 3, 2010, Secretary Napolitano, announced a series of initiatives to support state and local law enforcement and community groups across the country in identifying and mitigating threats to their communities by expanding the "If You See Something, Say Something" campaign to the Washington, D.C., area in conjunction with National Night Out, an annual anticrime campaign involving citizens, police and neighborhood groups.

In order to provide additional law enforcement training and resources to support local efforts to prevent future acts of violence, DHS has committed to:

- Working with federal partners and state and local law enforcement organizations to develop an innovative **community-oriented policing curriculum** for state and local law enforcement, focused on better enabling frontline personnel to distinguish between potential criminal and legal activities;
    - These groups include the Department of Justice, Los Angeles Police Department's Counter Terrorism Training Academy, the Naval Post Graduate School, the Major City Chiefs Association, the International Association of Chiefs of Police, and subject-matter experts
- Providing training through a variety of venues which will include DHS's Federal Law Enforcement Training Center, regional community policing institutes and online.

To increase public participation/awareness and preparedness about signs of criminal activity and violent extremism:

- DHS continues to expand its national **"If You See Something, Say Something" campaign** in coordination with law enforcement, the private sector, and community groups, integrating this effort with the Nationwide Suspicious Activity Reporting Initiative and the transportation, sports, travel, and law enforcement sectors.

To increase public participation/awareness and preparedness about cybersecurity:

- DHS created the challenge "**STOP. THINK. CONNECT.**" This challenge asks the public to create and upload short videos that will inspire Americans to be vigilant about developing safe online habits. The winning video will be posted on the 'STOP.THINK.CONNECT' website. More information about the challenge is available online at http://blog.dhs.gov/2010/11/stopthinkconnect-campaign-launches.html.

To improve information sharing/collaboration with law enforcement partners:

- DHS will produce a series of **unclassified case studies** examining recent incidents involving violent crime and terrorism to educate and inform state and local law enforcement personnel and community members about common behaviors and indicators exhibited by the suspects.

- DHS will produce **a series of intelligence products** regarding tactics, techniques and plans of international and domestic terrorist organizations—including the recruitment and training of individuals living in the United States – to better inform state and local law enforcement personnel about threats facing the homeland and their local communities.

To collect and share best practices with local law enforcement partners:

- DHS began a series of **regional summits** beginning in fall 2010 with state and local law enforcement, government, and community leaders to receive firsthand information and feedback on successful community-oriented policing and other crime reduction programs. DHS will **gather and share these case studies and best practices** with law enforcement partners nationwide using the widely-used *Lessons Learned Information Sharing* online platform.

- DHS and the Department of Justice will **publish guidance and recommendations** for state and local law enforcement agencies about ways to expand information sharing, suspicious activities reporting and identifying behavior that may indicate planning or other pre-operational indicators of criminal or terrorist activities. This agency-level guidance will serve as a complement to the individual officer curriculum.

To better collaborate with law enforcement partners at all levels:

- Because these new initiatives and policies are inherently relevant to local community partnerships, DHS will **expand cultural outreach and engagement activities** through its Office for Civil Rights and Civil Liberties (CRCL) in order to help both DHS employees and state and local law enforcement partners better understand, identify and mitigate threats.

To better engage the diverse communities affected by DHS activities:

- CRCL is aggressively staffing its public engagement office to enable them to better engage in regular outreach efforts with stakeholders across the country. The Engagement Teams or (E-Teams) will help improve outreach and engagement initiatives with American Arab, Muslim, Sikh, South Asian, Somali, Middle Eastern, and other ethnic and religious communities.

VI. Flagship Open Government Initiatives

Flagship Initiative 1.0 Virtual USA

In the Department's first Open Government plan, the Department selected Virtual USA (or vUSA) as its Flagship Initiative. vUSA is an innovative information-sharing initiative that draws on practitioner input to help Federal, State, local and Tribal first responders collaborate to make fast, well-informed decisions. vUSA integrates existing frameworks and investments to provide real-time access to operational information—such as weather conditions, traffic, the location and operational status of critical infrastructure, fuel supplies, availability of emergency shelters and medical facilities, and other critical information—that allows users to improve situational awareness and to respond quickly in emergencies. The Department utilized vUSA during the Deep Water Horizon Oil spill response in conjunction with other federal entities and declared vUSA a success

Flagship Initiative 2.0 National Information Exchange Model

The Department's second major initiative is the National Information Exchange Model (NIEM) (www.niem.gov). NIEM is a federal, state, local and tribal interagency initiative providing a foundation for seamless information exchange. Launched on February 28, 2005, through a partnership agreement between the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS) and signed by their Chief Information Officers, NIEM seeks to leverage the data exchange standards efforts successfully implemented by GLOBAL and extends the Global Justice XML Data Model (GJXDM) to facilitate timely, secure information sharing across the whole of the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprise.

Providing immediate access to timely, accurate and thorough information, and sharing critical data at key decision points are key objectives of the NIEM program.

Transparency

In the same way that technology standards like HTML enabled the dawn of the first generation of Web 1.0 applications, more advanced smart tagging technologies like XML have become critical to enabling this next generation of Web 2.0 platforms. These tagging technologies are critical to transparency initiatives and to feeding the evolving regulatory architectures of the Federal government.

The leading implementation of XML across the Federal government is NIEM. NIEM is also the commanding standard for State and local government collaboration with Federal departments. NIEM emerged out of a partnership between Department of Justice and Department of Homeland Security to strengthen cross-agency collaboration by adopting common XML data-tagging standards when exchanging data across jurisdictions.

NIEM tagging has become common practice for government agencies to connect data across their mission critical applications and on their Web 2.0 smart applications. The success of NIEM has recently led ten additional Federal agencies to commit to adopting the program. With that, the focus of NIEM has branched from national security and law enforcement mission spaces into becoming a standard approach for tagging government transparency data and is expanding to support secure health information exchanges.

Adoption of NIEM across various new domains continues unabated, but perhaps the most noteworthy examples of success are those which are inherently intergovernmental, made possible by NIEM. One such instance is the use of NIEM as the reporting standard for Recovery Act data from the states. The American Recovery and Reinvestment Act ("Economic Stimulus Act" or "Recovery Act") of 2009 established specific mandates for government transparency, accountability and openness particularly to counter waste, frauds abuse, or mismanagement of recovery funds. This was a union of opportunity and requirement, as the states, in particular through the National Association of State Chief Information Officers (NASCIO), were seeking consistent guidance across federal agencies in the format and mechanism of reporting Recovery Act results. It is important as adoption increases that the NIEM program continues to engage its strategic partners in the field to identify such opportunities for improvement.

Collaboration

NIEM represents a working and collaborative partnership directed by key governmental agencies and supported by operational practitioners, technologists, systems developers, private sector solution providers, and stakeholders in federal, state, local, and tribal governments.

Participation

In 2010, the NIEM program hosted a town hall in Washington, DC. The event brought together over 100 stakeholders to discuss the challenges and future priorities of the NIEM program.

During the town hall, facilitators led the group of participants through several questions related to NIEM. The exercise allowed attendees to engage and network with other stakeholders while producing over 550 ideas for consideration in the development of NIEM's 2011-2013 strategic plan. Participant input from the event was analyzed by the NIEM PMO, and some consistent themes were identified. This input is being used to form action plans for NIEM in the coming year. The full collection of ideas from the town hall is available through the NIEM public website: http://www.niem.gov/pdf/NIEM_TownHallRecap.pdf.

Flagship Governance Structure

The NIEM Executive Steering Council (ESC) is designed to provide executive leadership, vision, direction, and fundamental support for the NIEM program. The ESC sets policy and strategy, secures funding and appoints key personnel to the NIEM PMO. The ESC advocates for NIEM at senior levels of government and among key constituencies. Membership of the ESC is composed of federal

agency signatories of a memorandum of understanding (MOU) for NIEM users who have officially agreed to participate in and support NIEM.

NIEM PMO is the operational arm for NIEM. The Executive Director is appointed by the ESC and is responsible for execution of the vision defined by the ESC, strategic planning to support the program, and day-to-day management and operations.

The NIEM Business Architecture Committee (NBAC) is designed to guide the development, harmonization, evolution, and implementation of NIEM core data components and operating processes from a business architecture perspective. The committee is led by a chairperson and vice chairperson who coordinate their work with the NIEM Business and Outreach Director; it is supported by staff resources provided by the NIEM PMO Sponsoring Agency. Committee members are appointed by the NIEM PMO, in consultation with the ESC, key stakeholders, and representatives of engaged COIs.

The NIEM Technical Architecture Committee (NTAC) is designed to address technical and structural details associated with NIEM development and implementation. This committee is led by a chairperson. It is staffed by the NIEM Technical Architecture Director and supporting staff. Committee members are appointed by the NIEM PMO (in consultation with the ESC) and include the Policy Advisory Panel, key stakeholders, and representatives of engaged COIs.

The NIEM Communications and Outreach Committee (NC&OC) is designed to ensure that information regarding NIEM is consistently and effectively presented to key decision makers, agency executives, legislative and elected officials, investors, practitioners, agency representatives, and relevant COIs that include local, state, tribal, and federal entities, as well as the general public.

Flagship Initiative 2.0: National Cybersecurity Awareness Campaign

Every day Americans are incorporating new and innovative technologies into their lives. This exposure has increased the Nation's dependence on computers, smart phones and other online resources at home, at work and at school. The growing reliance on technology, coupled with the increased threat of malicious cyber attacks and loss of privacy, has given rise to the need for greater security of our lives online.

The very technologies that empower us to be more efficient, to multi-task, to manage our finances, and to communicate with family and friends also empower those who can invade, disrupt and destroy the worlds we've created for ourselves online. As we continue to evolve our lives with technology, as our children speed by us online, the need to be more prepared, proactive and protected should be clear. Unfortunately this is often not the case and millions of Americans are not aware of or are choosing to ignore the implications of not protecting themselves online.

President Obama declared cybersecurity one of the most serious economic and national security threats the nation faces. Working together, businesses, community-based organizations, the

American public and the U.S. government, can rise to the challenge and create innovative ideas to improve our nation's cybersecurity.

The U.S. Department of Homeland Security is working with organizations such as the National Cyber Security Alliance, to help families understand the importance of cybersecurity and that we all must share the responsibility of working together to improve our personal cybersecurity as well as the security of our nation's cyberspace.

Everyone has a stake in cybersecurity and we want to hear from you – whether you're a parent, high school or college-aged student, business executive, government employee or you work for a non-profit – you all have ideas that are relevant and meaningful and could be part of the solution to keeping our cyberspace safe.

As we develop messages in partnership to reach all Americans, we want the benefit of your ideas. How would you and your colleagues, friends, parents and children like to learn more about staying safe from cyber threats? The aim of this challenge is to gather and share the best, most creative ideas for making the public more aware and proactive when it comes to cybersecurity.

Transparency

The nature of the National Cybersecurity Awareness Campaign or any campaign for that matter is to be transparent and share messaging, resources, and recommendations with the public. The Campaign is set up to be a two-way communication vehicle between government and the public sector to share ideas that are relevant and meaningful and could be a part of the solution to keeping our cyberspace safe. All information, messages, resources, and tips and recommendations will be available to the public through a website owned and operated by DHS.

Collaboration

The National Cybersecurity Awareness campaign is the first track of a larger program, the National Initiative for Cybersecurity Education (NICE), stemming from the White House 60 Day Cyberspace Policy Review administered through the National Institute of Standards and Technology (NIST). NICE cuts across several Federal departments and agencies, including Homeland Security, the Department of Defense and the Department of Education. The Campaign includes public initiatives ranging from general public challenges to “friends of the campaign” grassroots initiatives. The Campaign is dedicated to Open Government concepts and has and will continue to solicit the best ideas available from both the public and private sectors.

Participation

The National Cybersecurity Awareness Campaign Challenge was launched by Secretary Napolitano at the RSA Convention in March 2010 to solicit cybersecurity public education awareness proposals from interested parties. DHS was fortunate to receive more than 80 submissions from individuals, universities and consulting firms. The seven winners were announced at the White House with White

House Cyber Coordinator Howard Schmidt, Secretary Napolitano, and Secretary of Commerce Gary Locke.

After the successful completion of the National Cybersecurity Awareness Campaign Challenge in March 2010, DHS decided to launch a follow-up for online PSAs. Participants will be asked to submit either 30 second or 60 second PSAs for distribution to our target demographics - teens, families and senior citizens - via social media networking sites. Guidelines are relatively flexible but each submission has to include one to five tips for cybersecurity and must incorporate the "Stop. Think. Connect." messaging that was developed in collaboration with a public/private messaging convention.

Flagship Governance Structure

In addition to using national programs for Campaign messaging, DHS will also utilize "Friends of the Campaign" to engage the general public at the grassroots level. A series of toolkits and training resources will be rolled out in the coming months. "Friends" will be asked to raise awareness of local cybersecurity vulnerabilities, leading at least one Campaign activity per year and identifying key personnel and celebrities in their area to further spread the Campaign message.

The Cybersecurity Awareness Campaign is dedicated to Open Government and engaging the general public on a variety of issues. The recent success of the National Cyber Challenge demonstrates that public solicitations can provide strong proposals from the very audiences DHS is targeting. Through the upcoming online PSA challenge and the "Friends of the Campaign" program, DHS will continue to open the process to the public and solicit the best ideas available.

National Strategy for Trusted Identities in Cyberspace

The Department launched the National Strategy for Trusted Identities in Cyberspace via IdeaScale and invited the public, academia and the private sector to participate in the Dialogue on the draft strategy.

The National Strategy for Trusted Identities in Cyberspace focuses on the protection of the identity of each party to an online transaction and the identity of the underlying infrastructure that supports it. This Strategy seeks to improve cyberspace for everyone – individuals, private sector, and governments – who conduct business online. The draft strategy report can be found online at http://www.dhs.gov/xlibrary/assets/ns_tic.pdf.

Appendix A –Response to National Public Dialogue

Idea Scale

The Department engaged the American public throughout the congressionally mandated Quadrennial Homeland Security Review (QHSR) process in 2009. The QHSR team conducted online *National Security Dialogues* (www.homelandsecuritydialogue.org), which were open to the public and subject matter experts across the country, to outline the strategic framework of homeland security toward a common end. Public dialogue about the QHSR recognized the roles and responsibilities of DHS, but also the relationships, roles, and responsibilities of homeland security partners.

The Department conducted another dialogue to hear from the public about their expectations for open government in an effort to understand what the public expects, and how the Department can best protect the nation and serve the public. Using a tool developed by the General Services Administration (GSA), the Department received over 100 ideas from the public and Federal employees on ways to make DHS more transparent, participatory, collaborative, and innovative.

The Department plans to utilize public dialogues to garner insight on topics of interest to a broad cross-section of the American Public.

DHS Response to National Public Dialogue comments

The Department solicited comments on the first version of its Open Government Plan using the GSA IdeaScale collaboration tool from April 30, 2010 through May 10, 2010. The Department received over 100 comments and suggestions through the National Dialogue on Open Government and selected the ten best and provided the following responses.

Preparation is Not a Dirty Word

Public Idea: DHS needs to put out comprehensive instructions for preparing for different disasters. Natural and man-made disasters occur someplace daily but those who would prepare are characterized as crazy people. The job of helping after any sort of disaster is improved if victims are not in a state of total devastation. The only way that can be avoided is to prepare in advance. We Americans are not used to having to prepare, therefore guidance is necessary. The guide currently available on the DHS website is inadequate for an event lasting 3 days. Our local Red Cross advisor was ill prepared when the hurricanes hit a few years ago, illustrating the need for guidance.

Response: DHS provides comprehensive instructions for preparing for different disasters via the *Ready* Campaign, information on websites, and an array of free publications. *Ready* Campaign's messages are distributed through: television, radio, print, outdoor and Internet public service advertisements (PSAs) developed and produced by the Advertising Council. Publications include *Are You Ready?* a comprehensive 200-page workbook on citizen preparedness and brochures and other materials for specific audiences such as the elderly, children, and people with disabilities. FEMA managed websites with available preparedness information include www.ready.gov, its Spanish-language version www.listo.gov, www.citizencorps.gov, and www.fema.gov. FEMA also maintains

toll-free phone lines 1-800-BE-READY and 1-888-SE-LISTO and a warehouse facility from which the public can order publications free of charge. The warehouse telephone number is 1-800-480-2520 (M-F: 8:00 a.m. - 5:00 p.m. est).

FEMA also works with state and local partners to create collaborative planning groups at the grassroots level to bring community and government leaders together to involve community members in all-hazards emergency preparedness, planning, mitigation, response, and recovery. These Citizen Corps Councils work to provide critical localized preparedness information to residents of the community on community plans and protocols. Citizen Corps Councils provide local residents with opportunities for training and volunteer service, including Community Emergency Response Teams (CERT), Fire Corps, Volunteers in Police Service, Neighborhood Watch, and Medical Reserve Corps. Find Citizen Corps Council locations on www.citizencorps.gov.

Information Sharing

Public Idea: The sharing of timely information important to critical infrastructure by federal agencies is a fallacy. We're told time and again that various security clearances are needed before information can be shared. As an InfraGard member, I'm asked to report suspicious or unusual activity; a one-way street. My suggestion is simple. Make obtaining various security clearances less onerous to obtain and direct those agencies that collect information regarding critical infrastructure responsible for engaging in two-way communication that is beneficial to both. Information is power only when it's shared.

Response: The Department grateful for this comment and suggestions regarding the improvement of two-way information sharing and communication between DHS and the Critical Infrastructure and Key Resources (CIKR) owner/operator community. Information sharing is a priority for the Department of Homeland Security (DHS) and accordingly, DHS continuously reviews its communication policies, processes and procedures to identify ways to improve two-way communication that is beneficial to both DHS and the private sector. In fact, the DHS Sector Partnership model is based upon the philosophy that creating and enhancing two-way communications between DHS and the CIKR owner/operators is essential to protecting the homeland. As the President noted in of the National Security Strategy,

> "The ideas, values, energy, creativity, and resilience of our citizens are America's greatest resource. We will support the development of prepared, vigilant, and engaged communities and underscore that our citizens are the heart of a resilient country. And we must tap the ingenuity outside government through strategic partnerships with the private sector, nongovernmental organizations, foundations, and community-based organizations. Such partnerships are critical to U.S., success at home and abroad, and we will support them through enhanced opportunities for engagement, coordination, transparency, and information sharing."

This continues to be a priority for the Department of Homeland Security.

The security clearance process established and administered by the Office of Personnel Management (OPM), is applied consistently across the board to all security clearance candidates, whether Federal government employees or private sector representatives. OPM is taking steps to streamline its processes for granting security clearances to make them less onerous. To obtain a security clearance, an individual must be in a position that requires a clearance and be sponsored by a government entity or a contractor with a security clearance. The entire process can take up to 18 months or more, depending upon the necessity of other record checks and reference interviews. Admittedly, the entire process can be cumbersome. It is, nevertheless, necessary and or minimize the risks of providing access to classified information to someone who may wish to harm to the United States.

Within the private sector realm, DHS works closely with the private sector representatives to identify the most appropriate candidates for security clearances in light of the standards set forth above. It is important to note that the purpose of sponsoring a CIKR community representative for a security clearance is to seek their input on the types of information which will be most useful to provide to the broader sector community and in no way should be regarded as an advantage over those who do not have a security clearance. The sectors nominate CIKR owners/operators to the government for clearances, based upon their positions within their companies and their sectors and then DHS IP sponsors the security clearance application. To date, approximately 1000 people, consisting of the CIKR owner/operator community, representing associations and companies across the 18 private sector industries have been granted security clearances. These security clearances fall within the SECRET category. There are also efforts under development to secure TOP SECRET security clearances for several representatives from each of the 18 private sector industries.

Yet another mechanism that is being used to facilitate CIKR owner/operator security clearances is the Fusion Centers. Located in most states and in major cities across the country, Fusion Centers were created to promote and facilitate information sharing and intelligence within their respective jurisdictions as well as with the federal government. To this end they are used to not only to provide expertise, coordinate with local law enforcement and other agencies, and provide local awareness and access, they also enable the flow of classified and unclassified information. As such, DHS is working with the Fusion Centers to develop a system that fosters a smooth process for security clearance nominations and processing, which also delegates appropriate responsibilities for training and oversight.

Although DHS will continue to work to increase the number of security clearances for our private sector partners, having a security clearance is not absolutely necessary for personnel to receive information that they need. Any tactics, techniques, and procedures that might be used in an impending attack, and that are identified in a classified document, will be appropriately downgraded to the point they can be shared with larger communities of CIKR owners/operators. Specific or detailed information about an impending terrorist attack, which is collected by agencies regarding critical infrastructure, is always shared with an intended or potential target, regardless of the clearance status of personnel at that site.

Benchmarking content on other agencies' FOIA pages

Public Idea: Most other federal agencies have FOIA web pages that contain a much richer amount of information than what is found on the FOIA page of DHS.gov. DHS should benchmark against peer agencies and add content commonly found on such agencies' websites, e.g. staff manuals and statements of policy - both of which are commonly found on other agencies' sites but neither of which are available on DHS.gov.

Response: The Department regularly updates and augments its FOIA Electronic Reading Room, as do the DHS components, and has adopted a policy of proactively disclosing certain categories of documents to increase agency transparency. Many records, such as the types cited in this comment (e.g. staff manuals and statements of policy) can be found on Departmental and component Web sites. A few examples of the types of records you can find on the main DHS.gov/foia site are ten volumes of DHS Directives and Instructions, (comprising 171 individual records), policy memoranda (such as those issued by the Chief FOIA Officer), privacy compliance documentation (such as SORNs and PIAs) and more. The Open Government Directive issued by OMB required that agencies post their FY09 Annual FOIA Report to the Attorney General on the Web in "open" format; DHS not only published FY09, but also published all prior years' annual FOIA reports in open format to assist the public. Furthermore, requesters can find many categories of frequently requested records on DHS.gov/foia, such as Departmental and component FOIA logs from 2009 through present, Inspector General records, procurement records and the Secretary's calendars. The DHS FOIA team works closely with DHS Web Publishing to post records as they become available. We encourage the public to send suggestions on how better to organize the FOIA Web site to make it more user-friendly to FOIA@dhs.gov.

Post TSA rules

Public Idea: Passengers going through TSA checkpoints are required to follow rules that are not spelled out in law or regulation but rather in documents claimed by DHS to be SSI. Secret laws are clearly un-American. Post the rules that passengers are required to follow to the web.

Response: TSA regulations clearly describe passengers' responsibilities at the checkpoint (49 C.F.R. Part 1540 Subpart B "Responsibilities of Passengers and other Individuals and Persons"). TSA also publishes a "What to Know Before you Go" forum on its website, www.tsa.gov. This has information for passengers about what items are prohibited, liquid rules for carry-on baggage, what to know if you are a traveler with a disability and many other topics. The Standard Operating Procedures that contain Sensitive Security Information (SSI) are procedures addressed to TSA staff, not passengers, and they contain information that would be damaging to security if terrorists had access to it. Members of the traveling public can not only find what they need to know on the TSA website, they can also ask Transportation Security Officers at security checkpoints for guidance on what to do.

Internal transparency

Public Idea: One problem with trying to share information to the public is that lower level employees may not be actually interfacing with the big picture. Many are given directives that are disconnected with the true day-to-day activities that are taking place in the fields. I was recently asked on an interview what were the core values of my agency. I was familiar with the core value rhetoric however; I was out of the loop as far as to be able to recite the values. I spent some time looking for them on the intranet but without success. This is an example of how there is still a very large disconnect between the overriding principals and activities of our agencies and it workers. I believe that if more emphasis is placed on work life issues employees will themselves take more of an interest in acquiring and implementing new information and policies and feel confident in sharing it with the public.

Response: Earlier this spring, the Department launched a single Intranet for the entire agency. This platform is a vast improvement in how the Department communicates and collaborates across the Department and at all levels.

Cybersecurity: Consolidated Zero-Day Citizen Reporting Portal

Public Idea: DHS should partner with commercial companies and government agencies to provide a consolidated portal for citizen reporting zero day vulnerabilities in both proprietary and open source code.

Citizen reports should be relayed to both national CERTs and the companies or communities respond for patching the vulnerability. All reports should be logged into a secure central system managed by the government, similar to how NHTSA manages vehicle reports. The government should require any vulnerability reported directly to commercial companies to be logged into this system as well.

On a regular basis, the government should produce a report on submitted cases. This report would be extremely high-level and would in no way compromise national security. Instead, it would serve to inform the American public of the state of cybersecurity in a more granular manner.

The portal would be designed to expand to include a social resource center offering: 1)a wiki with information on public vulnerabilities and links to third party software updates; 2) a forum for discussions around cybersecurity between citizens and government personnel.

Response: The Department of Homeland Security (DHS) is currently sponsoring the National Vulnerability Database (NVD) program, which already compiles vulnerability submissions. DHS is also standing up a new portal to comply with the public's comments; however, this would not necessarily simplify the process of vulnerability reporting or be a good example of IT infrastructure re-use. Modifying the current NVD to accept anonymous or attributed submissions of vulnerabilities found by public citizens could be more productive. With the modification to the NVD, there could be a requirement that any vulnerability reported directly to commercial companies should also be reported via the NVD submission process mentioned above. Additionally, a high-level report

detailing the current state of vulnerabilities could be produced and made available either for download or via a Security Content Automation Protocol (SCAP)-compliant model, which could be utilized by SCAP-compliant tools. Through the NVD portal, information on public vulnerabilities could be provided and links to commercial vendors' update sites should be maintained. This would provide U.S. citizens, Federal, State, local, tribal, and international entities a one-stop shop for this information.

The Department is now available to all employees in one standard place. This functionality is a great resource for staying up-to-date with Department events, initiatives, news and programs.

Also, all Department messages - from press releases, major speeches, transcripts, blog posts, Leadership Journals and event notifications – is available on www.dhs.gov.

More Public Awareness

Public Idea: I believe making the public more aware of possible terrorist and/or terrorist threats will assist budget and personnel strapped law enforcement agencies to leverage off the public sector. Shows like, "Americas Most Wanted", have assisted law enforcement in catching criminals. Request you explore using this type of medium to let people know, you need help.
Other Public awareness programs are: Crime Stoppers (which offer awards), tiplines, and Billboards announcements. Putting out information vice having them search for information, will keep the public informed plus, make people more aware of possible terrorism/crime.

Response: Since Secretary Napolitano came to the Department she has stressed the importance of shared responsibility and engaging the public to help fight terrorism and terrorist activities. Currently, an awareness campaign that addresses this idea is being developed to harness the shared goals of safety among communities, the private sector and all levels of government.

Increase public participation family emergency plans

Public Idea: Less than 10% of the overall population has taken the time to create a family emergency plan. This is even after the recent tragedies in Haiti, as well as other natural disasters around the world and in the United States. Take into consideration that over the last 20 years tens of millions of dollars has been invested in trying to get citizens to create a family emergency plan. Unfortunately, the success rate of getting people to actually create one is dismal. If you were working for a company, and only achieved 10% of your customers after tens of millions of dollars investment, you would not have a job.

This is not to say, that everyone involved in trying to get people to create a family emergency plan, where bad people, or that the idea and benefits of having emergency plan in the reduction of reliance of the first responders was a bad idea, it is just simply "everything" that has been tried, has failed to Garner greater than 10% of the population actually taking the time to create one.

The benefits, of a family having a family emergency plan cannot be disputed in regards of assisting in the prevention of loss of life and property through having a plan, including such basic things as making sure that children and others within a home know what to do in case there is a fire, as well as for natural and man-made disasters what to do in case one happens, how many times do you see the scenario play out on your television new screen, that children or others have died in apartment fires or home fires, where the percentage of these tragedies could be avoided by simply training those affected what to do in case there was a fire, a greater percentage of those that died may not have died had the of known what to do. A perfect example, and what motivated me to attempt to tackle this problem, in February of 2009, in Graham Washington, there was an apartment fire. In this fire a 14-year-old girl actually made it out of the burning apartment, then realizing that her 8 year old little brother was still inside she went back in to that burning apartment to rescue her 8-year-old brother and unfortunately died in the apartment fire with him. I would stake my life on the fact that if this 14-year-old girl, and her 8-year-old brother had been trained that if there was an apartment fire the first thing that they should attempt to do is try to grab each other's hands if possible on the first attempt of exiting the burning apartment. No one will actually know if this would have saved their lives, but using common sense I personally feel that those 2 children may not have lost their lives had their parents taken the time to give them a basic understanding of what to do should there be in apartment fire.

Along those lines, you might be able to understand as I do, that a family emergency plan encompasses not only things like apartment fires or home fires, but those things that are local to a family such as natural or man-made disasters with the natural disasters planning being based upon the area in which they live (for example, a snow evacuation route would most likely not be needed in Miami Florida).

There are many good people such as faith-based organizations, NGO (nongovernmental organizations) and nonprofits, as well as local first responder groups that have attempted over the years to guide people in the creation of family emergency plans. The failure has been not in the training presentations that these individuals have provided, nor in the resources handed out at those events, at fault, is in the fact that most of the individuals receiving these resources simply take them home, and never fill them out.

I believe, there is a methodology and a process, that can change the perception of family emergency planning, that raises the level of priority in an average citizens mind, the importance of their participation in creating a family emergency plan for their families.

You can say that there are many, many reasons why people do not take the time to create a plan, yet when you ask people why they have not created one, you still get a "deer in the headlight" look from them.

One of the most prevalent reasons I believe people have lost creating a family emergency plan as a priority, is the ongoing loss of community participation. Technology has been one of the items that has destroyed traditional community involvement. For example, what used to be a method in the 60s 70s and 80s of people doing community-based things, were like friends getting together at a

restaurant or a bowling alley and discussing things face-to-face. Technology, simply by its nature reduces this activity "why drive down to the restaurant and bowling alley to talk with your friends, when you can just jump online and chat with them, or send your ideas out via twitter, Facebook etc.

I believe that there is a way to leverage technology to bring that community aspect and participation back into the fold, yet preserve the traditional methods of getting together on community efforts for those that do not have technology, as a combined effort to compel people to create family emergency plans.

During the Haiti earthquake response, I witnessed an amazing thing, in less than a week, the world tried to come together in response to that natural disaster, including recording artists, actors etc. utilizing the media, and technology to generate a monetary response to assist them in recovery. So I know, people really do care, however, do they care enough to protect themselves and their families by reducing their risk by being prepared? I believe also, that if presented correctly, and everyone gets behind the idea, via media and technology such as we witnessed in the response to the Haiti natural disaster we can in fact affect a change in culture and increase compelling families to create family emergency plans.

As a parting thought, historically again I remind you, that everything that has been done before on this path, has failed to get greater than 10% of the population in the states and internationally to take the time to create a family emergency plan, this to me is absolute failure.

I invite any challenges to this, anyone having any ideas, those having contacts with the movie star and popular recording artists, to come together, and help make this a priority, by doing so, if this activity saves one child's life from burning up in apartment fire, (I believe it will save more), and the reduction of the stress on the first responders (without families being prepared and knowing what to do during a natural or man-made disaster, they will call 911, and expect a response, unfortunately they will not get one because the first responders are already overwhelmed) the benefits of doing this if thought of with common sense could be dramatic in the assistance of preventing loss of life and property.
Thank you for your time,

Response: According to a 2009 *Ready* Campaign survey, 56% of Americans have a family emergency plan. The *Ready* Campaign's core messages (Get a Kit, Make a Plan, Be Informed) emphasize the importance of creating a family emergency plan. There are family emergency plan templates available on ready.gov and listo.gov (Spanish-language version).

In 2009, the *Ready* Campaign introduced a series of new social media tools to further engage Americans in taking steps to prepare for emergencies. At the center of the initiative is a Web page, "Be Prepared," which features an interactive widget that provides users with updates on emergency situations, local emergency contact information, an instructional video, emergency kit checklists and guidelines on how to better prepare for an emergency. The program also includes a tool with which visitors can create their own comprehensive Family Emergency Plan and share important information with their family and friends.

In addition to stressing the importance of having a family plan, FEMA has also conducted significant research on personal preparedness, including national household surveys in 2003, 2007, and 2009. During the 2009 National Conference on Community Preparedness, the Federal Emergency Management Agency (FEMA) released a new report *Personal Preparedness in America: Findings from the 2009 Citizen Corps National Survey* that offers comprehensive data on the public's thoughts, perceptions, and behaviors related to preparedness and community safety for multiple types of hazards. Findings from these surveys provide valuable insights for increasing personal preparedness, civic engagement, and community resilience.

Results from this study have important implications for the development of more effective communication and outreach strategies to achieve greater levels of preparedness and participation. Suggested strategies based on this data include:

Stress that preparedness is a shared responsibility. Results from the national survey indicate that 29 percent of Americans have not prepared because they think that emergency responders will help them and that over 60 percent expect to rely on emergency responders in the first 72 hours following a disaster. While government will execute its functions, communications to the public should convey a more realistic understanding of emergency response capacity and emphasize the importance of self-reliance. Messaging should speak to a shared responsibility and stress that everyone has a role to play in preparedness and response.

Provide more specificity on preparedness actions. This research also found that many people who report being prepared have not completed important preparedness activities or do not have a sound understanding of community plans. Of those who perceived themselves to be prepared, 35 percent did not have a household plan, 77 percent had not conducted a home evacuation drill, and 73 percent did not know their community's evacuation routes.

Highlight additional preparedness needs for people with disabilities. Fifteen percent of respondents reported having a physical or other disability that would affect their capacity to respond to an emergency situation. Alarmingly, however, few individuals with disabilities had taken specific actions to help them respond safely in the event of an emergency. Only 28 percent had taken a CPR or first aid training and less than half (47%) had a household plan. Another 14 percent of survey participants indicated they lived with and/or cared for someone with a physical or other disability. Of these individuals, 37 percent reported taking CPR training, 40 percent reported taking first aid training and 54 percent had supplies set aside in their home.

Emphasize the importance of drills and exercises. Practicing response protocols is critical for effective execution; this is true for emergency responders and true for the public. Fewer than half the surveyed individuals (42%) had practiced a workplace evacuation drill, only 14 percent had participated in a home evacuation drill, and of those in school and/or with children in school, only 23 percent had participated in a school evacuation drill. And the numbers are much lower for shelter in place drills (27%, 10%, and 14% respectively). Drills and exercises for multiple hazards and multiple locations need to be conducted through social networks. In addition, community members need to be included more effectively in government-sponsored community exercises.

Offer specialized information on the survivability of manmade disasters. These results indicate that individuals' perceived utility of preparing and their confidence in their ability to respond varies significantly by disaster type. Only 6 percent of individuals felt that nothing they did would help them handle a natural disaster, whereas 35 percent felt nothing they did would help them in an act of terrorism, such as a biological, chemical, radiological, or explosive attack. All-hazards terminology may mask important nuances relative to conveying personal preparedness guidance for specific hazards. It is important to emphasize the survivability of manmade disasters and the relevant protective measures for these hazards.

Couple a national voice with local specificity. National leaders must be strong advocates for personal preparedness, but it is clear that messages specific to individual preparedness must include critical local information, such as information on local hazards, local alerts and warnings, and local community response protocols. Local social networks must also be used to support outreach and education on personal preparedness, such as neighborhoods, the workplace, schools, and faith communities. And the concepts of mutual support at the local, neighborhood level should be emphasized.

FEMA's Citizen Corps grassroots community resilience movement and the Ready.gov awareness campaign work together to actively involve Americans in making themselves and their communities safer, stronger, and better prepared to handle any emergency situation. 2,400 local communities nationwide have created Citizen Corps Councils to strengthen collaboration between government and civic leaders and to educate, train, and involve the public. For more information about Citizen Corps, visit www.citizencorps.gov. To learn more about the Ready.gov Campaign, visit www.ready.gov.

To read the survey reports, go to http://www.citizencorps.gov/ready/2009findings.shtm.

Explanations for Delays in Rule Making Process

Public Idea: Congress has mandated through the legislative process that DHS develop a variety of new rules and regulations. In many cases DHS has significantly missed the mandated dates by which they were supposed to have published the final rules; for example: the ammonium nitrate security rule (RIN 1601-AA52) and the security training for freight railroad employees rule (RIN 1652-AA57). While there is almost certainly a good reason for the delay in the rule making process, there is no public accountability for the delays.

To help increase the transparency of the regulatory process, I would like to suggest that DHS establish a regulatory progress web page listing each legislatively mandated rule or regulation that has yet to be published in its final form. The web site could then list the current status of each rule and the reasons for the delays (if any) in getting the final rule published.

Response: DHS recognizes the importance of keeping the public apprised on the status and substance of regulations that the Department and its components promulgate. To that end, the Department points out that there are mechanisms in place to facilitate the sharing of that information. Of note, DHS, along the other federal regulatory agencies, publishes the Unified Agenda of Regulatory and Deregulatory Actions ("Unified Agenda") twice per year, usually in April and November. The

Unified Agenda summarizes the rules and proposed rules that DHS expects to issue in the coming year. The entries for the rules include, among other things an abstract summarizing the rule, an indication of whether there is a legal deadline associated with that rule, and a timetable of the next actions for that particular rule. Prior to 2007, the Unified Agenda was published in the Federal Register. Beginning with the fall 2007 edition, the complete Unified Agenda is now available online at Reginfo.gov. (Agencies continue, however, to publish in the Federal Register entries for those rules which are likely to have a significant economic impact on a substantial number of small entities or rules that have been selected for periodic review under section 610 of the Regulatory Flexibility Act.) In addition, each Fall, DHS (along with the other federal agencies) prepares a Regulatory Plan narrative, which describes the most important significant regulatory actions that DHS reasonably expects to issue, in proposed or final form, in the coming fiscal year. The Regulatory Plans of all federal agencies, including DHS, are published together in the Federal Register each fall.

Make communication a priority

Public Idea: Regarding USCIS: Promote communication with the general public regarding the status of their cases, thus thwarting undue stress and frustration. Rather than just letting their case status sit at "Initial Review" for 4+ months.

Add a category for "background check initiated", or "case awaiting priority date". Anything to ease the frustration of having to wait for months to be reunited with a loved one.

Response: Thank you for this question. We agree this is an issue that causes significant confusion for our customers and we have been working to take corrective action. The best and final answer lies in the USCIS Transformation effort. Our Transformation team is working to create an entirely new automated system that will positively affect every aspect of the application process and the customer experience. One benefit of the transformed USCIS is that it will allow applicants and their advocate's ready access to USCIS and will proactively provide detailed information about the status of benefit requests. The first phase of our Transformation will be deployed in mid 2011 and rollouts will continue for two years after that. In the meantime, USCIS continues to try to improve communication around an applicant's case status. Recently, USCIS implemented the new My Case Status tool online at USCIS.gov. This tool allows customers to track the status of their application as it moves through the adjudications process. My Case Status provides a description of activities undertaken by USCIS while the case is in process. These activities can be viewed by placing your mouse over the applicable action. For example, background check and fingerprint activities are included within the Initial Review selection. Further enhancements will be rolled out in July that will, in certain circumstances, allow applicants to deal directly with the office adjudicating their application and provide case status updates and facilitate Change of Address in Spanish. We are currently evaluating the displaying of a pre-adjudicated status on My Case Status for cases that have been reviewed and approved by USCIS but require visa issuance from the Department of State.

Appendix B - DHS Data.gov Pipeline

Source	Component	Idea or suggestion	Stage
DHS	CBP	CBP Airport Wait times - Seasonal Monthly Average	1. Discovery
DHS	CBP	List of Pre Clearance Locations	1. Discovery
DHS	CBP	List of Port Of Entries by Land, Air and Sea	1. Discovery
DHS	CBP	CBP Border Wait Times	1. Discovery
DHS	CBP	Record of Vessel in Foreign Trade Entrances	1. Discovery
DHS	CBP	FOIA Requests	1. Discovery
Public	CBP	Historical Border Wait Times by Port of Entry, Mode of travel (e.g., pedestrian, motor vehicle, truck, SENTRI), month, day of week, time of day	1. Discovery
Public	CBP	Data on the location and time of illegal border crossings and drug seizures	5. Not Feasible for Release
Public	CBP	US Port seizures	1. Discovery
Public	DHS	Department of Homeland Security Threat level over time.	1. Discovery
DHS	DHS CFO	Budget and Finance Documents	1. Discovery
DHS	FEMA	Pre-Disaster Mitigation Projects Summary	1. Discovery
DHS	FEMA	Public Assistance Project-level dataset	8. Data Online
DHS	FEMA	Hazard Mitigation Program Summary	8. Data Online
DHS	FEMA	Public Assistance Funded Projects Summary	8. Data Online
DHS	FEMA	Disaster Declarations Summary	8. Data Online
DHS/ Public	FEMA	Flood Hazard Maps	8. Data Online
DHS	FEMA	Public Assistance Grant Program Trends	1. Discovery
DHS	FEMA	2009 Disaster Statistics	1. Discovery

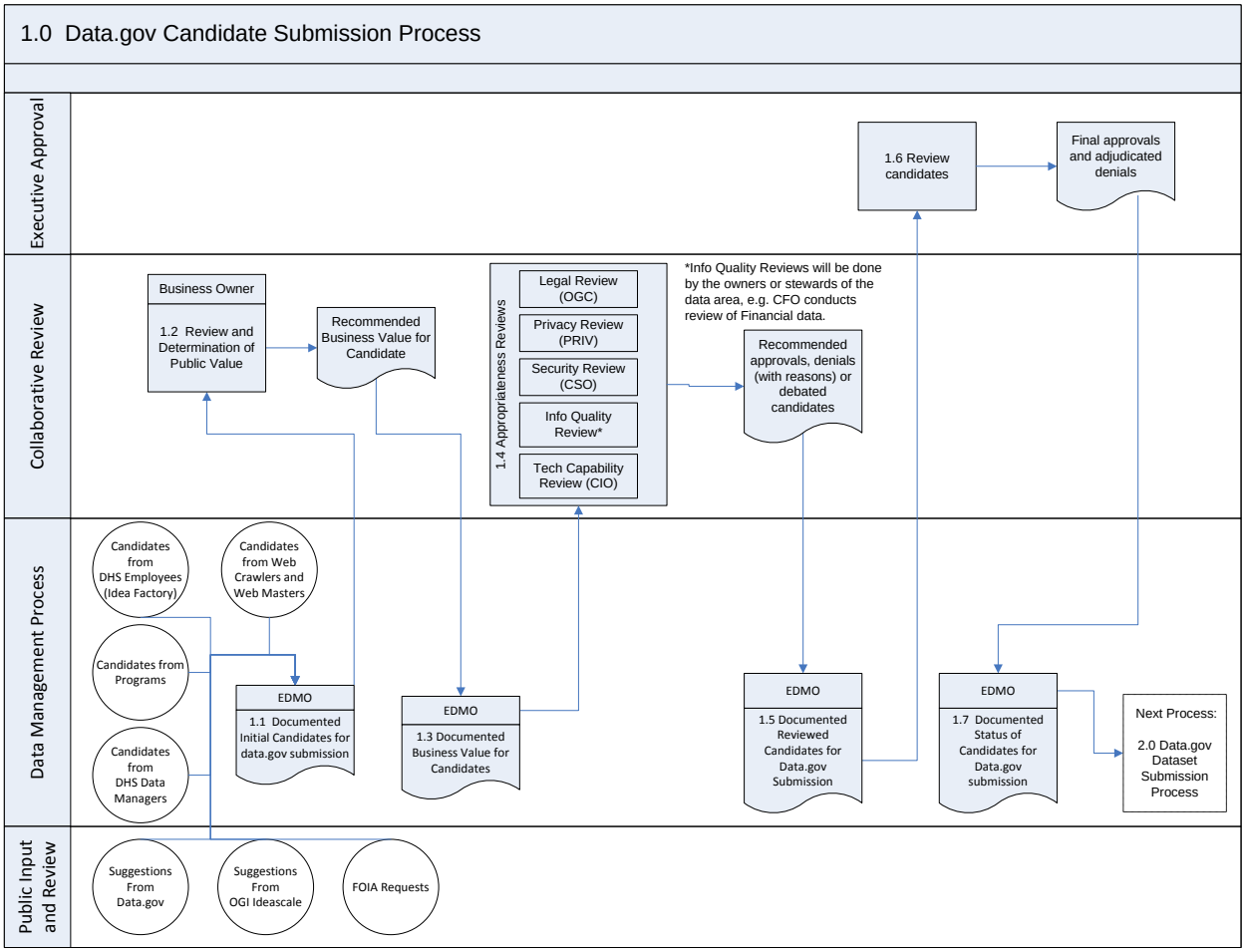
Source	Component	Idea or suggestion	Stage
Public	FEMA	Disaster-related data (could be its own dataset) would be of great value. In the short-term, data such as cost per disaster or numbers of Americans who registered for aid could be distributed. In the long-term, as data from FEMA is screened for personal, sensitive information (such as addresses, etc), data could be released for academic study (such as income levels, averages of grants to various socio-economic levels, etc)...	1. Discovery
Public	FEMA	What can FEMA or DHS provide in terms of individual assistance aggregate data, public assistance aggregate data, presidential disaster declaration data, etc. There are well over 100 educational programs in the U.S. with multiple graduate programs - students and faculty are searching for data for theses, dissertations and publications. Thanks.	1. Discovery
Public	FEMA	Dollar figures for homeland security grant spending awards by state and government entity.	1. Discovery
Public	FEMA	Grants from 1999 to 2009	1. Discovery
Public	FEMA	Building Fire and Research Laboratory data from research and experiments.	1. Discovery
DHS	FLETC	Student Statistics (enrolled, graduated, …)	3. Preliminary Review
DHS	ICE	Detention and Removal Statistics	1. Discovery
DHS	ICE	Arrest statistics	1. Discovery
DHS	ICE	Intellectual Property Rights Seizure Statistics	1. Discovery
DHS	ICE	Student and Exchange Visitor Information System	1. Discovery
Public	ICE	US Port seizures	1. Discovery
DHS	NPPD	LandScan USA	5. Not Feasible for Release
DHS	NPPD	HSIP Freedom Geo-layers (160+)	5. Not Feasible for Release
DHS	OHA	Health Security Index	3. Preliminary Review
DHS	OHA	Health Security Scoring	8. Data Online
DHS	OIG	Investigations / Audits	1. Discovery

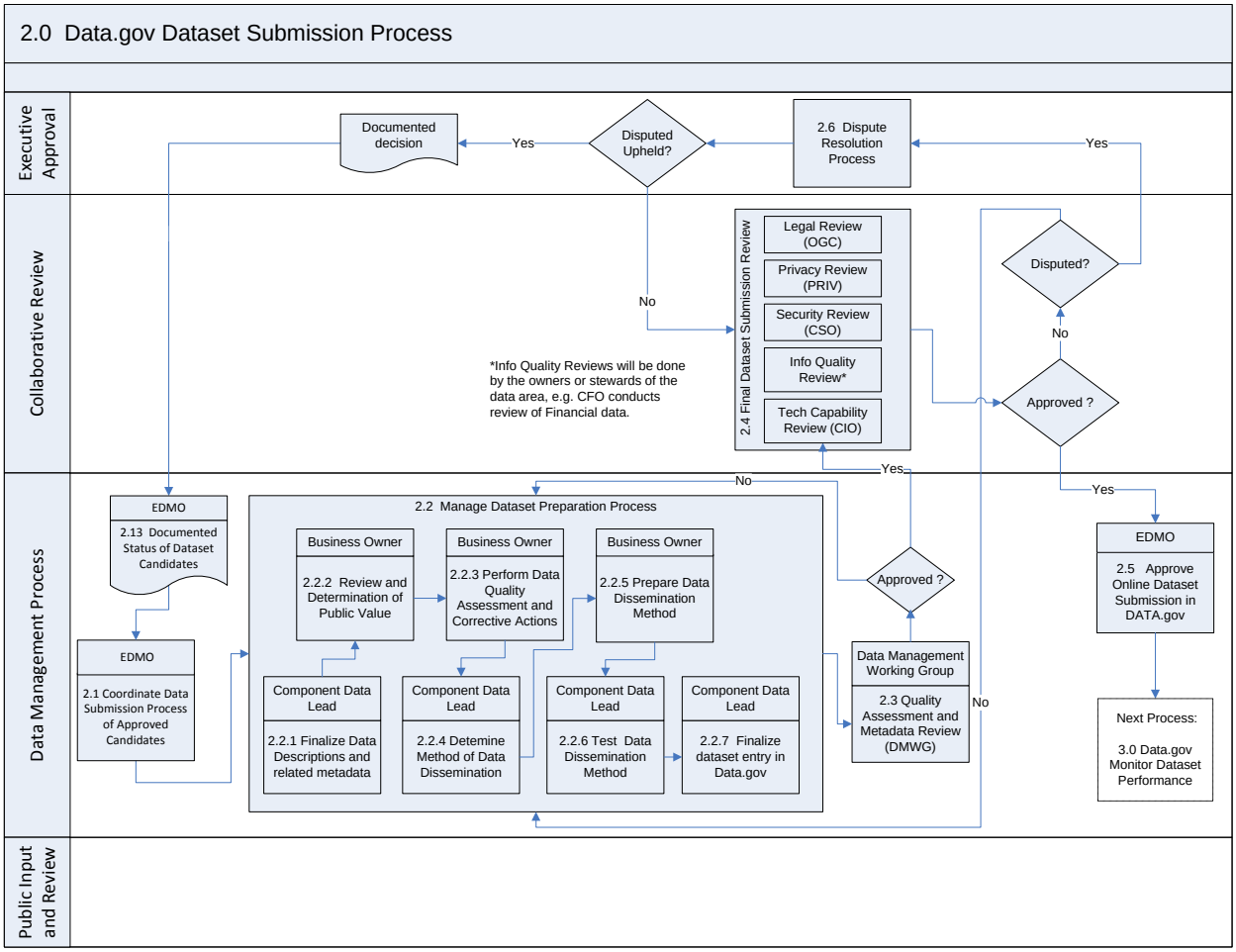
Source	Component	Idea or suggestion	Stage
DHS	S&T	Research Investments / Outcomes	5. Not Feasible for release
DHS/ Public	TSA	Damaged Baggage Claims	2. Definition
DHS	TSA	Civil Rights Complaints	1. Discovery
DHS	TSA	Traveler Redress	1. Discovery
DHS	TSA	Firearms Confiscation	2. Definition
DHS	TSA	Artfully concealed prohibited items found at checkpoints	2. Definition
DHS	TSA	Historical Transportation Security Fee Collection Data	1. Discovery
Public	TSA	Racial profiling in airports to prevent terrorism	5. Not feasible for release
Public	US CERT	The public and unclassified data from the Worldwide Incidents Tracking System published by the National Counterterrorism Center on its web site, wits.nctc.gov.	1. Discovery
Public	US CERT	I'd like to see DHS/CERT publish lists of IP addresses that attack government networks on a daily basis.	1. Discovery
DHS	USCG	Marine Casualty and Pollution	4. Final Review
DHS	USCG	Merchant and recreational vessels	5. Not Feasible for Release
DHS	USCG	U.S. Coast Guard Search and Rescue Statistics	1. Discovery
DHS	USCG	Port State Information Exchange (PSIX)	5. Not Feasible for Release
Public	USCG	US Port seizures	1. Discovery
Public	USCG	Federal Information Clearinghouse of Marine Debris Information	1. Discovery
Public	USCG	Do you have any information on how the Coast Guard spends their money? In particular, their construction projects.	1. Discovery
DHS	USCIS	FOIA Requests	8. Data Online

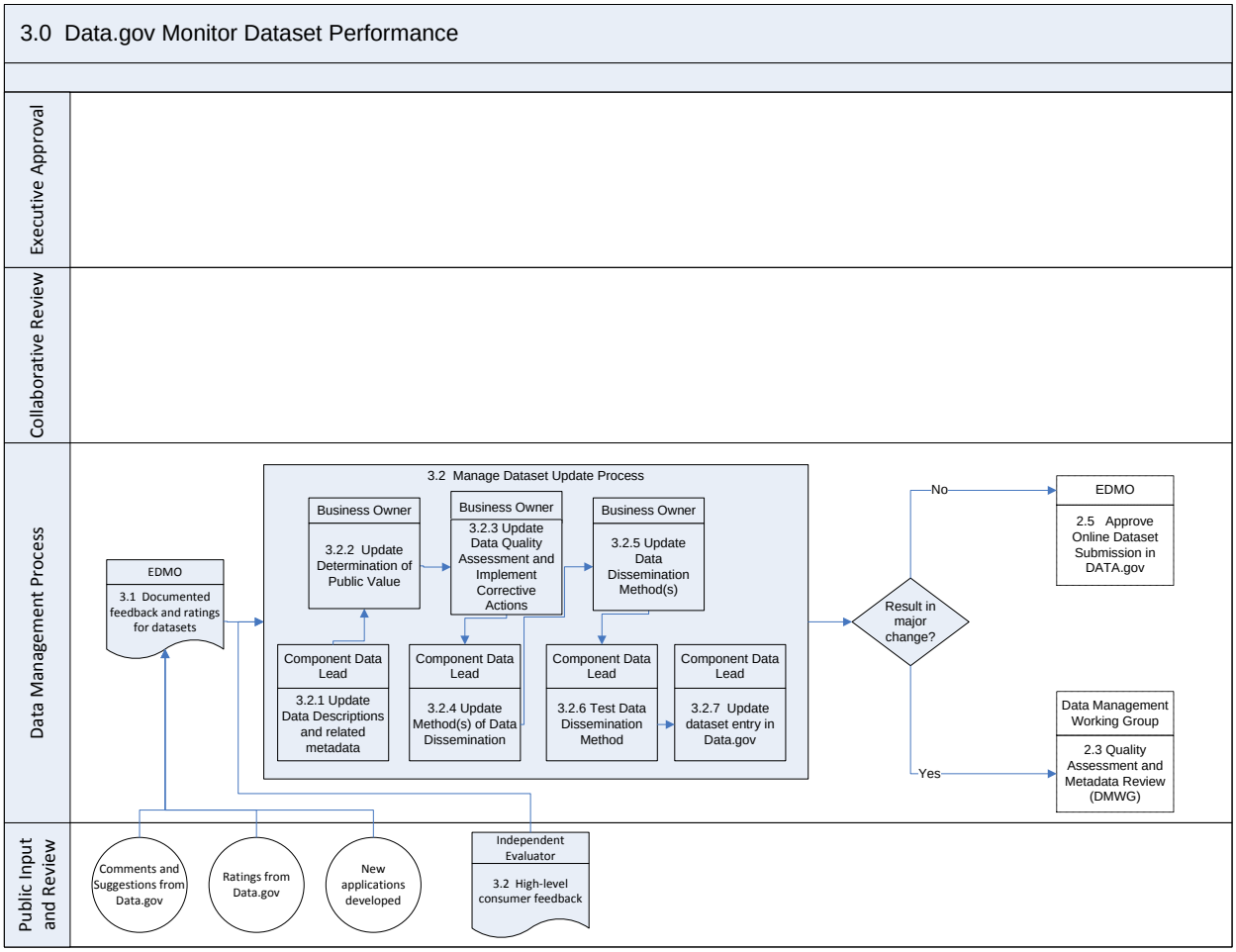
Source	Component	Idea or suggestion	Stage
DHS	USCIS	Equal Employment Opportunity Data Posted Pursuant to the No Fear Act	1. Discovery
Public	USCIS	USCIS - Immigrant and non-immigrant data, case processing status data.	1. Discovery
Public	USCIS	Immigration Subset = Legal | Illegal	5. Not Feasible for Release
Public	USCIS	immigration status, finger print, green card,	1. Discovery
Public	USCIS	Immigration, laws, policies enforcement, changes in the last 50 years	5. Not Feasible for Release
Public	USCIS	Real time immigration data. Number of visas issued of all types. Diversity visa data	1. Discovery
Public	USCIS	Immigration statistics and how that relates to the population of Hispanics in the U.S. How many Mexican-Americans move back and forth between the two countries? Or how many baby boomers are retiring in Mexico?	5. Not Feasible for Release
Public	USCIS	Temporary immigration H-1B occupational characteristics L-1 occupational characteristics	1. Discovery
Public	USCIS	It will be great if USCIS post current backlog for Highly skilled immigrants waiting for green card based on their Priority date	5. Not Feasible for Release
Public	USCIS	N-400 Application for Naturalization processing times (by center) RSS feed	8. Data Online
Public	USCIS	I would like to see data about pending/approved/rejected green card applications by country and family/employment category.	1. Discovery
Public	USCIS	USCIS? Immigration Department data, Helps legal immigrants to know when to expect green cards and citizenships	1. Discovery
Public	USCIS	emigration	5. Not Feasible for Release

Source	Component	Idea or suggestion	Stage
Public	USCIS	Every month DOS/USCIS publishes Visa Bulletin, which describes who are eligible to get Green Card, but then they don't mention how many visas are used or are available for the current fiscal year instead the mighty word used is "DUE to HIGH LOAD". It would be great to have that data available so for the folks waiting for visa availability, this data might give more transparency as to what DOS/USCIS is doing.	5. Not Feasible for Release
Public	USCIS	The United States Citizenship and Immigration Services (USCIS) maintains monthly statistical data in the form of the PAS (Performance Analysis System). It is raw monthly data from each USCIS office of the number of applications received and processed. It does not contain personally identifiable information or national security sensitive information. However, the excel spreadsheet format of the information makes it easy to use and it is the best available current data on USCIS receipts and processing nationwide. The release of this important information will make the agency more responsive to the public especially since it is a fee authorized (and not an appropriated agency).	1. Discovery
DHS	USSS	Criminal Investigation statistics	5. Not Feasible for Release

Appendix C - Data.gov Collaborative Review Process




2.0 Data.gov Dataset Submission Process
Executive Approval
Collaborative Review
Data Management Process
Public Input and Review
Documented decision
Yes
Disputed Upheld?
2.6 Dispute Resolution Process
Yes
No
*Info Quality Reviews will be done by the owners or stewards of the data area, e.g. CFO conducts review of Financial data.
2.4 Final Dataset Submission Review
Legal Review (OGC)
Privacy Review (PRIV)
Security Review (CSO)
Info Quality Review*
Tech Capability Review (CIO)
Disputed?
No
Approved ?
Yes
No
Yes
EDMO
2.13 Documented Status of Dataset Candidates
2.2 Manage Dataset Preparation Process
Business Owner
2.2.2 Review and Determination of Public Value
Business Owner
2.2.3 Perform Data Quality Assessment and Corrective Actions
Business Owner
2.2.5 Prepare Data Dissemination Method
Component Data Lead
2.2.1 Finalize Data Descriptions and related metadata
Component Data Lead
2.2.4 Detemine Method of Data Dissemination
Component Data Lead
2.2.6 Test Data Dissemination Method
Component Data Lead
2.2.7 Finalize dataset entry in Data.gov
EDMO
2.1 Coordinate Data Submission Process of Approved Candidates
Approved ?
Data Management Working Group
2.3 Quality Assessment and Metadata Review (DMWG)
No
EDMO
2.5 Approve Online Dataset Submission in DATA.gov
Next Process:
3.0 Data.gov Monitor Dataset Performance


3.0 Data.gov Monitor Dataset Performance
Executive Approval
Collaborative Review
Data Management Process
Public Input and Review
3.2 Manage Dataset Update Process
EDMO
3.1 Documented feedback and ratings for datasets
Business Owner
3.2.2 Update Determination of Public Value
Business Owner
3.2.3 Update Data Quality Assessment and Implement Corrective Actions
Business Owner
3.2.5 Update Data Dissemination Method(s)
Component Data Lead
3.2.1 Update Data Descriptions and related metadata
Component Data Lead
3.2.4 Update Method(s) of Data Dissemination
Component Data Lead
3.2.6 Test Data Dissemination Method
Component Data Lead
3.2.7 Update dataset entry in Data.gov
Result in major change?
No
EDMO
2.5 Approve Online Dataset Submission in DATA.gov
Yes
Data Management Working Group
2.3 Quality Assessment and Metadata Review (DMWG)
Comments and Suggestions from Data.gov
Ratings from Data.gov
New applications developed
Independent Evaluator
3.2 High-level consumer feedback

Appendix D- Dataset Governance for Data.gov

Data.gov allows DHS to rate datasets and provide feedback. The feedback is used to refine datasets and provide any additional information that may make the dataset more useful. The number of downloads and rating by the public are used to determine if a dataset has been of value to the public. The DHS datasets shown in the following table were originally published in June 2009 to support the release of Data.gov.

Persons Obtaining Legal Permanent Resident Status by Region and Country of Birth: Fiscal Years 1999 to 2008 Access data on immigrants who became legal permanent residents in fiscal year 2008 by class of admission, country of birth, state of residence, and other characteristics	(1 votes)
Persons Obtaining Legal Permanent Resident Status by Type and Major Class of Admission: Fiscal Years 1999 to 2008 Access data on immigrants who became legal permanent residents in fiscal year 2008 by class of admission, country of birth, state of residence, and other characteristics	(1 votes)
Immigrant Orphans Adopted by U.S. Citizens by Gender, Age, and Region and Country of Birth: Fiscal Year 2008 Access data on immigrants who became legal permanent residents in fiscal year 2008 by class of admission, country of birth, state of residence, and other characteristics	(5 votes)
Persons Naturalized by Region and Country of Birth: Fiscal Years 1999 to 2008 Access data on persons who became American citizens in fiscal year 2008 by country of birth, state of residence, and other characteristics	(1 votes)
Persons Obtaining Legal Permanent Resident Status: Fiscal Years 1820 to 2008 Access data on immigrants who became legal permanent residents in fiscal year 2008 by class of admission, country of birth, state of residence, and other characteristics	(3 votes)
Persons Obtaining Legal Permanent Resident Status by Leading Core Based Statistical Areas (CBSAs) of Residence and Region and Country of Birth: Fiscal Year 2008 Access data on immigrants who became legal permanent residents in fiscal year 2008 by class of admission, country of birth, state of residence, and other characteristics	(2 votes)
Individuals Granted Asylum Affirmatively or Defensively: Fiscal Years 1990 to 2008 Access data on persons admitted as refugees or granted asylum in fiscal year 2008 by several characteristics.	(1 votes)

Datasets published on Data.gov are intended to be updated at an interval appropriate for the data, quarterly or monthly. If a dataset raises no concerns during the review process, updates to the dataset are not reviewed unless the structure of the dataset is changed, e.g. a new field is added or the type of data in a field is changed. If concerns or issues are identified during the review process, each update to the dataset is reviewed to ensure that it meets the standards for publication.

Appendix E - Transparency in American Recovery and Reinvestment Act

The Department of Homeland Security received $2.75 billion through the American Recovery and Reinvestment Act (ARRA) appropriation. This money was distributed across 15 programs within six Components and offices. Unlike other federal agencies, the bulk of DHS awards are contracts, and nearly all awards, whether contracts or grants, are competitively awarded.

American Recovery and Reinvestment Act (ARRA)

($Amounts in millions)

DHS Headquarters	$200
U.S. Customs and Border Protection (CBP)	$680
U.S. Immigration and Customs Enforcement (ICE)	$20
Transportation Security Administration (TSA)	$1,000
U.S. Coast Guard (USCG)	$240
Federal Emergency Management Agency (FEMA)	$610
Office of the Inspector General (OIG)	$5
TOTAL DHS ARRA	**$2,750**

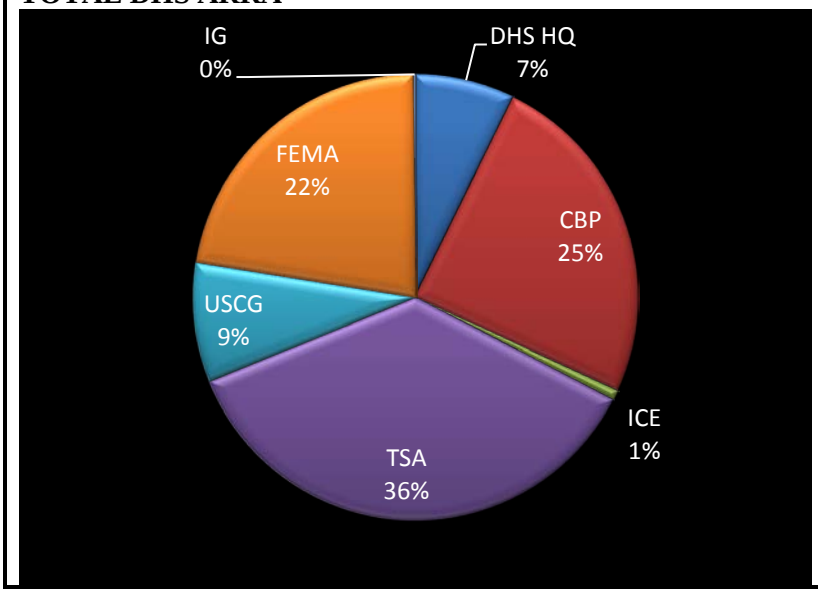


Figure 3- DHS ARRA allocation

As of 30 September 2010, the Department obligated over 97% of its funds and is on track to have awarded 100% of funds by the end of the calendar year 2010. Our outlays are rapidly ramping up as many of the infrastructure projects graduate from the design phase to construction phase.

When Congress passed the Recovery Act, it wanted the American people to be able to track where the dollars are spent and how those dollars impact individual communities. In order to achieve this level of transparency, Congress included reporting requirements for both the Federal Agencies and the award recipients. Congress mandated that www.Recovery.gov be built as a repository for all ARRA reports. Each week DHS Components provide program level financial updates for posting to the

Recovery.gov site. In addition, every week the Department delivers a report to the Office of Management and Budget (OMB) that contains all new awards. The purpose of this report is to notify businesses of sub-contracting opportunities in their areas.

DHS also created a department recovery page, www.dhs.gov/recovery, where members of the public can learn about DHS-specific programs and track the Department's progress in obligating funds and auditing work. A mapping tool, currently in the test phase, will allow users to visualize where DHS awards are making an impact.