Open Government Plan 2016 - 2018

U.S. Department of Homeland Security

Homeland Security

Message from the Deputy Under Secretary for Management

In an on-going effort to support the Open Government efforts, I am pleased to release the Department of Homeland Security's (DHS) 2016 Open Government Plan. This plan builds upon the success of the past, and focuses on how the principles of Open Government support the DHS mission. The vision for Open Government was outlined in President Obama's 2009 Memorandum on Transparency and Open Government, and the follow-on Open Government Directive from the Office of Management and Budget (OMB). Throughout his Administration, the President has prioritized making government more open and accountable, and has taken substantial steps to increase citizen participation, collaboration, and transparency in government.

On July 14, 2016, the Open Government Directive (M-16-16) was issued, instructing executive departments and agencies to update current Open Government plans and ensure specific actions are taken to incorporate the principles of transparency, participation, and collaboration. With contributions from senior policy, legal, and technology leadership, the Department has updated its current Open Government plan to incorporate implementation plans for the new Open Innovation Methods, Scientific Data and Publications, Open Source Software, and Spending Information (DATA Act) initiatives.

DHS has identified a new flagship initiative that addresses openness, public participation, and transparency. The Global Travel Assessment System (GTAS) flagship initiative demonstrates the Department's continued commitment to combatting the threats of global terrorism and transnational crime. Additionally, updates to the Open Data, Freedom of Information Act (FOIA), and Public Participation have been provided.

DHS will continue to work with our public and private partners in increasing collaboration, ensuring public participation, and promoting openness that strengthens public trust.

OCT 2 1 2016

Chip Fulghum
Deputy Under Secretary for Management
Department of Homeland Security

Date

Table of Contents

I. Executive Summary

On July 14, 2016, the Office of Management and Budget (OMB) issued Open Government Directive (M-16-16), instructing executive departments and agencies to update current Open Government plans and ensure specific actions are taken to incorporate the principles of transparency, participation, and collaboration.

With contributions from senior policy, legal, and technology leadership, the Department has updated its current Open Government plan to incorporate implementation plans for the new Open Innovation Methods, Scientific Data and Publications, Open Source Software, and Spending Information (DATA Act) initiatives.

II. Background

After OMB released the Open Government Memorandum in 2009, the Secretary of Homeland Security designated the Management Directorate (MGMT) to lead the implementation of Open Government. In Fiscal Year (FY) 2010, the Deputy Under Secretary for MGMT signed the past Open Government plan.

Since the release of that plan, DHS has continued to build on its commitment to Open Government as demonstrated in subsequent updates.

This current plan reflects input from senior policy, legal, and technology leadership, and details the specific actions and commitments that DHS will undertake along with timelines for completion. The updated plan provides an overview of past accomplishments, status updates on major initiatives listed in preceding plans, and introduces new open government initiatives.

III. Open Government Governance

At the direction of the Deputy Under Secretary for MGMT, the Office of Chief Information Officer (OCIO), worked to address Open Government deliverables, evaluate how to best incorporate Open Government into the Department's processes, and establish performance measures to gauge the Department's progress in incorporating Open Government into its operations.

Data Management Working Group

The Data Management Working Group defines, promotes, and monitors Enterprise Data Management practices. Such practices achieve the objectives of information sharing, discovery and reuse for and within DHS. This working group enables DHS Components and partners to harmonize their enterprise data management decisions; promote the conditions for information sharing across DHS; identify data security, privacy and classification initiatives; and lay the foundations for extensible interoperability across the broader Homeland Security community.

Data Integrity Working Group

The Data Integrity Working Group is working across DHS on Data Quality improvements, including working closely with senior leaders engaged in procurement/acquisition actions and those engaged in financial assistance program administration. The working group works very closely with data stewards to ensure data sets are relevant to their intended uses, and are of sufficient detail and quantity, with a high degree of accuracy and completeness, consistent with other sources, and presented in appropriate ways.

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

IV. Contributing Offices

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

Privacy Office
The DHS Chief Privacy Officer ensures that technologies in operation at DHS do not violate privacy protections, that personal information contained in Privacy Act systems of record adhere to the Privacy of 1974, and evaluates legislative and regulatory proposals involving the collection, use, and disclosure of personal information by the federal government.

The Privacy Office accomplishes its mission by requiring compliance with federal privacy and disclosure laws and policies in all DHS programs, systems, and operations; providing leadership and guidance to promote a culture of privacy and adherence to the Fair Information Practice Principles across the Department; and ensuring transparency to the public through published materials, reports, formal notices, public workshops, and meetings.

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. The CFO provides oversight and guidance to ensure internal controls support the integrity of grant, loan, and contract information posted publicly on USASpending.gov, and that adequate internal controls are in place for that information.

Office of Public Affairs
The Office of Public Affairs (OPA) coordinates the public affairs activities for the entire Department and serves as the federal government's lead public information office during a national emergency or disaster. OPA leads the information flow about the Department and its missions to the public, media, and employees via multiple modes of communication with the public.

Office of Partnership and Engagement (OPE)
The Office of Partnership and Engagement (OPE) leads the Department's outreach efforts with external stakeholders ranging from governors, mayors, tribal officials, county officials, law enforcement, private sector and business leaders, academic institutions, and the national associations that represent all of these stakeholders. One of OPE's outreach efforts is the "If You See Something, Say Something™" public awareness campaign. The campaign enhances the public's awareness of suspicious activity related to terrorism and terrorism-related crime. To accomplish this, the campaign develops public awareness materials that encourage the public to report suspicious activity to the appropriate law enforcement authorities within their communities.

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. CRCL advises Department leadership and stakeholders with public policy creation and implementation, leads the Department's equal employment opportunity programs, and promotes workforce diversity and merit system principles. CRCL also communicates with individuals and communities whose civil rights and civil liberties may be affected by Department activities and informs them about avenues of redress. In addition, CRCL investigates and resolves civil rights and civil liberties complaints filed by the public regarding Department policies or activities.

Office of Legislative Affairs

The Office of Legislative Affairs (OLA) serves as primary liaison to members of Congress and their staff. OLA responds to inquiries from Congress, notifies Congress about Department initiatives, policies, and programs, and keeps Congress informed by providing timely information about Homeland Security and national security matters. OLA provides valuable information to Congress through briefings, testimony, and background information papers. OLA also provides staff discussions and field visits for members of Congress, or their staffs, to gain a better understanding of DHS operations.

V. Flagship Initiatives

DHS has a new flagship initiative that supports the new Open Source and Open Innovation Methods initiatives, and also supports the expanded Open Data initiative. The Global Travel Assessment System (GTAS) was made available to the public in July 2016, via the DHS GitHuB site at https://github.com/US-CBP/GTAS.

NEW FLAGSHIP: GLOBAL TRAVEL ASSESSMENT SYSTEM

U.S. Customs and Border Protection (CBP) is offering advanced passenger data screening and targeting technology as an open source software project. The purpose of GTAS provides foreign nation states, and border security entities, with the basic capacity to ingest, process, query, and construct risk criteria against their industry derived standardized air traveler information. This provides border security organizations with the necessary tool to prescreen travelers entering into and leaving their respective countries. GTAS has been developed and released by the Targeting and Analysis Systems Program Directorate within CBP, and it will be made available at no cost to the community at large. This applies to both commercial and government organizations who will be free to use, maintain, customize, and enhance as needed.

In response to the United Nations Security Council Resolution 2178 on Foreign Terrorist Fighters and CBP's continued commitment to combat the threats of global terrorism and transnational crime, DHS is evaluating and implementing innovative methods to exchange information and intelligence, build capacity, and increase worldwide security and compliance standards. Core GTAS capabilities include:

- Receive and store air traveler data [Air Passenger Information (API) and Passenger Name Record (PNR)];
- Perform real time risk assessment;
- View high risk travelers with associated flight details and reservation information; and
- Query flight and travel history.

An integral element of this mutually rewarding security collaboration between CBP and our international partners is our assistance with the development of programs, technology, training, and coordination efforts that will produce a seamless and layered network of capabilities. These efforts widen border security capabilities and support a "defense in depth" approach to combat the global threat environment, as well as strengthen our combined enforcement efforts.

GTAS is a turn-key application that provides all the necessary decision support system features to receive and store air traveler data (API and PNR), provide real-time risk assessment against this data based on a country's own specific risk criteria and/or watch lists, and view high risk travelers as well as their associated flight and reservation information.

GTAS was built upon a suite of open source licensed software components and platforms. As such, CBP licensed the GTAS software using the GNU General Public License. The open source GTAS code and resources are available to the public on GitHub at https://github.com/US-CBP/GTAS.

Updates to Previous Flagship Initiatives

FLAGSHIP: AUTOMATED COMMERCIAL ENVIRONMENT "SINGLE-WINDOW"

DHS CBP and 47 other federal agencies are involved in what has traditionally been a largely manual and paper-based trade process, which is costly and time-consuming for both the Government and the international trade community. Approximately 30 agencies have required over 200 forms for the importation and exportation of cargo.

On February 19, 2014, President Obama signed an Executive Order (EO), streamlining the Export/Import Process for America's Business. The 2014 EO ordered the streamlining of the import/export process by calling for the completion of a "single window" allows businesses to electronically transmit the data required by the U.S. Government to import or export cargo by December 2016. The Automated Commercial Environment (ACE) will become that "single window," the primary processing system through which the trade-related data required by all Government agencies is submitted and processed[1].

Through ACE, federal agencies have earlier, automated visibility to shipment data, which will expedite import or export assessments at the border and increase the flow of legitimate trade. Access to shipment data will also improve the security, health, and safety of cargo. Interactions between Partner Government Agencies (PGAs) will be automated to enable near-real time decision making, reducing costs for business and Government. ACE also promotes improved data quality which supports risk management and contributes to streamline processing.

CBP has already developed and deployed most core trade processing capabilities in ACE; these capabilities have streamlined business processes within federal government and industry. CBP and the PGAs have made steady progress on the implementation of ACE and single window filing capabilities and are on track to complete implementation by the December 2016 timeframe set forth in the Executive Order.

[1] Application forms for permits and licenses excluded from the Single Window.

FLAGSHIP: FEDERAL EMERGENCY MANAGEMENT AGENCY – OPENFEMA

Building off DHS's Open Government plan, OpenFEMA takes steps to proactively publish data sets in open formats that are easily accessed by citizens, the private sector, and non-governmental organizations.

OpenFEMA provides access to current and historical data, such as using FEMA's Open Data to More Effectively Rebuild after Hurricane Sandy. OpenFEMA will institutionalize programs and processes throughout FEMA, thus empowering program and regional offices to release data and engage with their external stakeholders to address needs unique to their communities.

FLAGSHIP: NATIONAL INFORMATION EXCHANGE MODEL (NIEM)

NIEM is jointly managed at an executive level by DHS, Department of Justice, and the Department of Health and Human Services. NIEM's governing structure is comprised of federal, state, local, tribal and private organizations. NIEM helps communities with common mission interests connect and exchange information in order to successfully and efficiently accomplish their missions.

NIEM focuses on the development of shared services using cross-organizational information exchange across multiple levels of government. All 50 states, the majority of federal agencies, including the Department of Defense, and the international community are committed to using the model in some capacity and at differing levels of maturity.

We can report the following key recent accomplishments:

- Onboarding of new domains to include military operations, human services, surface transportation, and agriculture;
- Participation in external working groups, such as the White House Data Cabinet;
- Establishment of partnerships with organizations, such as the National Association of State Chief Information Officers;
- Creation of tools that enable broader NIEM adoption through the JavaScript Object Notation, which is an open standard format that uses human-readable text to transmit data objects; and Application of geospatial capabilities and promotion of best practices in mapping to support key mission areas.

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

VI. New and Expanded Initiatives

Open Data

Enterprise Data Inventory

In compliance with OMB Memorandum M-13-13, DHS uses it's Enterprise Architecture Information Repository (EAIR), which is the centralized repository of Enterprise Architecture assets used by DHS and its Components. Each DHS Component is responsible for maintaining an accurate, up-to-date description of its data assets within the EAIR in accordance with DHS Directive Number 103-01 Enterprise Data Management Policy and as is documented in the Enterprise Data Management Concept of Operations.

DHS has been populating the EAIR with extensive data asset metadata since 2008 and associated over 95% of its systems to a corresponding data asset (4,248 of 4,451 operational systems associated). The EAIR currently includes approximately 1,547 data assets and sets of data with 34% being public. The published data assets are now undergoing a registration and certification process to identify authoritative and trusted data sources. The intent of certifying data assets as authoritative is to increase the reuse and confidence level in the data.

The information in the DHS EAIR includes security classification, privacy sensitivity, and handling restrictions such as For Official Use Only, Law Enforcement Sensitive, Special Security Information, and other types of Controlled-But-Unclassified categories. This categories includes non-government restrictions, such as data protected by trade agreements or those to protect intellectual propriety of private sector partners. Because of its homeland security and national security missions, the categorization of the data assets shows that only 35% of the 1547 data assets and datasets contain data that is releasable to the general public.

DHS Uses Open Data in the following ways:

(1) Further the Agency's core missions: When suitable, the release of publically available information greatly increases the public's awareness of DHS activities and fosters further positive interaction by allowing a multitude of perspectives and ideas to be brought to bear on existing problems and challenges. This greatly increases the reach of DHS in areas previously not identified. Various types of outreach channels are being utilized to make publically accessible data available. Because of the scope and nature of DHS, comprised of 22 large and small Components, the types of data and means of communicating such outreach will vary.

(2) Increase Agency accountability and responsiveness: Transparency in government operations provides another checks and balances on addressing issues forthrightly and responsively. The ability for the public to have a window into DHS operations ensures that the Department adheres to proper procedures in its operations and provides insight for possible areas for improvement.

(3) Increase Agency effectiveness and efficiency: DHS is able to tap into the innovation that is available in the public domain. By tapping into innovative new ideas and uncovering existing business models addressing similar challenges, DHS can accelerate its efforts toward effectiveness and efficiency.

(4) Spur innovation and collaboration: Access to the wealth of data collected by DHS and made accessible to the public has already been leveraged and combined with other tools to create innovative solutions. When leveraging FEMA raw data, geospatial tools such as Environmental Systems Research Institute (ESRI) can provide unique insights as to where emergency management resources should best be positioned in natural disaster situations, such as Hurricane Sandy. These innovative new cyber tools can be further leveraged by Components, such as FEMA, to improve their predictive processes for dealing with future disasters.

(5) Create economic opportunity: The types of innovative new tools created by leveraging DHS Open Data, in combination with entrepreneurs' skills at recognizing how to satisfy market needs, provides a powerful engine for economic opportunity and play into the strengths of America ingenuity.

A public data listing is available in the DHS section of Data.gov. DHS has added several new metadata fields to the Enterprise Data Inventory to allow the public data catalog to be extracted along with the data.gov metadata. A public access metadata field contains a drop down for Public, Public-Restricted, and Non-Public. All data assets and datasets marked Public and Public-Restricted in the DHS EAIR are extracted when the Public Data Catalog extract script is executed monthly or on the quarterly milestone date. The Public Data Catalog is updated with the agency and program values for each extracted row and converted to JavaScript Object Notation (JSON). The Data.JSON file is then published on the DHS Digital Strategy web page.

DHS has incorporated guidance and decision points into the engineering life cycle that encourage programs to consider all of the potential audiences and users of the data in a particular system and incorporate the process for data dissemination over the life of the system. Investment submissions are reviewed each year to determine if data dissemination is being addressed or improved.

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

Privacy Office:

eFOIA Mobile Application:
The Department continues to modernize and improve its FOIA operations by deploying advanced technology. The DHS Privacy Office partnered with OCIO to create the new eFOIA mobile application. In July 2015 the DHS Privacy Office launched the first, and currently only, government FOIA specific mobile application available for any iOS or Android mobile device. The application provides a consolidated resource of all FOIA related information pertaining to FOIA operations at DHS. By conveying the online request process to mobile devices, requesters can now submit requests and check the status of existing requests anyplace, anytime. Key features of the application allow users to: (1) submit a FOIA request to any DHS Component; (2) check the status of their requests; (3) access all of the content on the DHS FOIA website and library; and (4) view updates, changes to events such as stakeholder meetings/conference calls, and recently published documents.

After the first 12 months of the application launch it has received over 2,000 downloads. Metrics have shown that the application is being used, such as the check status capability that is receiving over 130 hits per month on average. Metrics have also provided valuable information as to areas where improvements can be made.

Currently our main focus is looking at the submission form and ways we can improve the user experience. Though the application offers a comprehensive FOIA submission form designed to help users provide complete FOIA submissions, existing functionality makes completing the form cumbersome on mobile devices.

We have received feedback from the requester community stating that the form in the application is not useful for those that submit multiple or frequent FOIA requests. Therefore we are looking at ways in which improvements can be made while maintaining user privacy. One such option would be the ability for users to opt-in to allow the application submission form to remember user contact information and save selections (radio buttons, yes/no questions, etc.) as template or default selections for that user. This will greatly reduce the number of clicks the user will have to make by eliminating the need to repetitively enter or select information thereby saving the user time.
For additional information, please visit: https://www.dhs.gov/efoia-mobile-app

Freedom of Information Act (FOIA) Requests
The Privacy Office ensures overall compliance with FOIA by developing Departmental policy needed to implement important FOIA initiatives, such as the sweeping changes set forth in the President's FOIA Memorandum and the Attorney General's FOIA Guidelines of 2009. Additionally, on June 30, 2016, President Obama signed into law the FOIA Improvement Act of 2016, which contains several substantive and procedural amendments to the FOIA as well as new reporting requirements for agencies.

The Privacy Office performs coordination and oversight of Component FOIA operations, provides FOIA training, and prepares mandated annual reports of the Department's FOIA performance. The Privacy Office, through its FOIA unit (hereinafter referred to as the DHS FOIA Office), also processes initial FOIA and Privacy Act requests to the Office of the Secretary (including the Military Advisor's Office and the Office of Intergovernmental Affairs), and eight DHS Headquarters Components (DHS FOIA Office Components).

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

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

For more information regarding DHS FOIA operations and processes, see the DHS Privacy Office 2016 Chief FOIA Officer Report:

[2] 5 U.S.C. § 552a.

https://www.dhs.gov/sites/default/files/publications/2016-chief-foia-officer-report-april-4-2016.pdf

Record Setting FOIA Requests

DHS consistently receives the largest number of FOIA requests of any federal department or agency in each FY, almost 40 percent of all requests within the Federal Government. Since President Obama took office, DHS experienced an increase in the number of received FOIA requests. In FY 2015, DHS received 281,191 FOIA requests, and processed 348,936 requests as compared to 238,003 last year. So far in FY 2016, DHS has received 230,135 requests and closed 205,958 requests through June 2016.

The volume of requests may be due to current events and the public interest in DHS missions and the activities of its components. Of particular public interest are immigration records in the possession of CBP, U.S. Immigration and Customs Enforcement (ICE), the Office of Biometric Identity Management (OBIM) within the National Protection and Programs Directorate (NPPD), and U.S. Citizenship and Immigration Services (USCIS). These Components continue to receive the largest number of requests, receiving 97%of all requests in FY 2015. To date, 96% of DHS FOIA requests were received by either NPPD, ICE or USCIS.The DHS Privacy Office remains committed to promoting transparency in DHS operations through timely and thorough processing of FOIA requests, reducing its backlog, and providing gold standard customer services and support.

The DHS Privacy Office issued a policy memorandum, Freedom of Information Act and 2015 Sunshine Week, in March 2015, highlighting some of the Department's accomplishments during the past year in furthering its openness and transparency initiatives. Although this memorandum was published during last year's reporting period, the DHS Privacy Office distributed this memorandum throughout this reporting period at training sessions. The memorandum is available at http://www.dhs.gov/sites/default/files/publications/priv-foia-2015-sunshine-week.pdf.

To improve customer experience, the DHS Privacy Office redesigned the online FOIA Library to include the libraries for the National Protection and Programs Directorate, the Federal Emergency Management Agency, and the Transportation Security Administration, making it easier to locate records disclosed by these Components.

Proactive Disclosure

In order to support the Open Government Directive, the Privacy Office has taken the lead in providing guidance for proactive disclosure of information. The Privacy Office maintains its commitment to transparency through the continued reduction of FOIA backlogs and increasing transparency through accessibility. Successes in Open Government for the Privacy Office include electronic reading rooms within DHS Operational Components, and a significant reduction in backlogged FOIA requests. The Freedom of Information Act outlines the transparency requirements government agencies must follow.

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

Open Innovation Methods

Science and Technology (S&T) Public Private Partnerships InnoPrize Program-Open Innovation through Prizes and Challenges

In support of open innovation methods as defined by the Open Government Directive and the 2015 Strategy for American Innovation, the S&T Public Private Partnerships Office developed the InnoPrize Program in October 2014 to support the Department's strategy to stimulate innovation, solve tough problems, and advance the agency's core missions through prizes and challenges. The Department recognizes crowdsourcing and prize competitions as a powerful tool for spurring innovation to address pressing challenges in homeland security. In addition, they serve as a valuable vehicle for mobilizing citizen scientists' technical talent, creative thinking and the entrepreneurial spirit that are the hallmarks of our nation.

In January 2016, The Department marked its first year of conducting prize competitions under the America COMPETES Act. Accomplishments include:

- Developing a Directive and Instruction for prize competitions;
- Dedicating a full-time S&T Senior Advisor for Crowdsourced Innovation;
- Conducting seven strategic, policy and training sessions for Components, leaders and program managers;
- Developing internal and external marketing and outreach;
- Developing and publishing a periodic newsletter, crowdsourcing development guidebook, dedicated SharePoint site and multiple program manager tools;
- Establishing a prize competition support contract under the GSA's Challenges and competition Services; and
- Planning and completing three crowdsourced prize competitions.

Crowdsourced Innovation Accomplishments-Year One

In March 2015, DHS announced the "**Where Am I, Where is My Team?" *Indoor Tracking of the Next Generation First Responder*** challenge to acquire fresh, unique approaches to the enduring problem of tracking first responders in GPS-degraded or denied environments. The ideas received through this challenge significantly informed S&T's research and development approach to tracking in development of a broader system of wearable technology for first responders.

S&T's Office of National Labs sponsored the "***NBAF-Think and Do Challenge***" to seek business plans that will improve the future National Bio and Agro-Defense Facility's (NBAF) mission of shaping and advancing bio/agro security. In order to capitalize on the benefits of the NBAF, S&T sought novel, smart strategies to advance the innovation, collaboration, training and talent of the facility. The challenge provided seed funding to build two new pieces of the bio-agro security innovation ecosystem—an ecosystem consisting of people, institutions, policies, and resources that will promote research.

S&T's Borders and Maritime Division and the USCG's Research and Development Center partnered to seek ***New Methods for Mooring Buoys in Environmentally Sensitive Areas***. The challenge, which drew the interest of hundreds of citizen scientists, sought solutions that would protect some of the most fragile aquatic habitats from documented destructive mooring and anchoring practices used

for decades. The winning idea, submitted by a native Hawaiian diver and makerspace organizer, provided a solution consisting of existing technologies that when integrated together will eliminate the destructive action of moving chains and lighter duty anchors common with today's buoys. The winning idea will be further developed and tested by the USCG and could become common practice throughout U.S. coastal waters.

Crowdsourced Innovation Activities Moving Forward in 2016-2018
In February 2016, the S&T Directorate partnered with NASA's Center of Excellence for Collaborative Innovation to develop new technology solutions through publically crowdsourced prize competitions. This partnership will provide access to end to end solutions on all aspects of implementing challenge-based prize competitions from problem definition to challenge design and administration. The agreement will also permit Component program managers to tailor their support requirements while providing access to leading experts in the prize competition field.

FY 2016-2018 Planned Crowdsourced Innovation Activities Include:

- Prize and Challenge Program assessment and improvement plan;
- Increased marketing and outreach;
- Workshops and training tailored to support Department Integrated Product Teams and Component challenges;
- Access to prize scientist consultation services;
- Planning and launching multi-phased and more complex challenges including working prototypes, algorithms, and applications; and
- Identifying and implementing citizen science projects throughout DHS Components.

The public can become a part of the DHS citizen science and crowdsourcing movement and receive future notification of DHS prize competitions by registering at https://www.challenge.gov/registration/. Features include:

- Share their areas of interest and skills;
- Communicate with DHS Prize Competition Managers;
- Participate in blogs and discussions; and
- Manage submitted solutions and submit solutions.

S&T Office of University Programs – Cooperative Research efforts
In support of the focus on collaboration as defined by the Open Government Directive, the Office of University Programs in the S&T Directorate has several Centers of Excellence (COE) that routinely work with DHS Components on developing analytical products and tools to improve the mission capabilities and efficiencies of DHS Components. This effort is closely monitored by the Directorate to ensure that data are adequately protected and used according to the Cooperative agreement or Basic Ordering Agreement. Managed through the Directorate's Office of University Programs, the COEs organize leading experts and researchers to conduct multidisciplinary homeland security research and education. Each center is university-led or co-led in collaboration with partners from other institutions, agencies, national laboratories, think tanks and the private sector. For additional information, please visit: http://www.dhs.gov/st-centers-excellence.

For additional information, please visit: https://www.dhs.gov/science-and-technology/prize-competitions.

Access to Scientific Data and Publications.

In 2013, the White House Office of Science and Technology Policy (OSTP) directed federal agencies that spend more than $100 million per year on research and development to develop plans to increase access to the results of unclassified research supported wholly or in part by federal funding. Such results include digital data and scholarly publications resulting from federally funded research (intramural and extramural).

Open Source Software

DHS supports the Federal Source Code Policy, and in April 2016 our Chief Information Officer was the only CIO of a Federal agency to publish comments in support of the policy: https://github.com/whitehouse/source-code-policy/issues/222.

We are currently working towards implementing this policy and launching new open source projects across DHS, such as GTAS, which is highlighted as a Flagship Initiative in this plan.

DHS is a strong supporter of open source software. We believe moving towards government-wide reuse of custom-developed code and releasing federally funded custom code as open source software has significant financial, technical, and cybersecurity benefits, and will better enable DHS to meet our mission of securing the nation from the many threats we face.

When managed appropriately, releasing code as Open-source software (OSS) and engaging with the community can have extensive cybersecurity benefits. Security through obscurity is not true security. We cannot depend on vulnerabilities not being exploited just because they have not been discovered yet.

There are many examples of widely-used pieces of software that benefit greatly from constant and vigorous community reviews and contributions to find bugs, and thus making them more secure. We look forward to government systems joining them. However, agencies should thoughtfully consider what components and libraries they release, and build active communities around their projects to ensure these benefits are realized. Without proper management and feedback from these communities, we believe the value of OSS is significantly diminished.

DHS looks forward to implementing this policy towards improving the way custom-developed government code is acquired and distributed in the future. Participation in the open source community will further strengthen our security systems and help fulfill the mission of the Department. Likewise, we believe in the potential of this policy to incentivize innovation and enable a new generation of companies to do business with the government.

Spending Information

When the Federal Funding Accountability and Transparency Act (FFATA) was passed in 2006, its goal was to increase accountability and transparency in federal spending. FFATA legislation required that information on federal awards (federal financial assistance and expenditures) was made available to the public via a single, searchable website, now known as www.USASpending.gov.

On May 9, 2014, President Obama signed the Digital Accountability and Transparency Act (DATA Act), which builds on FFATA by making information on federal expenditures more easily accessible and transparent. The law requires the U.S. Department of the Treasury to establish government-wide data standards for financial data and provide consistent, reliable, and searchable data on USASpending.gov.

One year after the act was signed, the Office of Management and Budget (OMB) issued formal guidance M-15-12 titled "Increasing Transparency of Federal Spending by Making Federal Spending Data Accessible, Searchable, and Reliable." DHS is required to report financial data in accordance with the new standards by May 2017. This includes linking obligations by appropriation, program activity, and object class with procurement and financial assistance award data.

A DATA Act Project Team within DHS was formed in March 2015. This group was charged with establishing, facilitating, and monitoring the process required to comply with this legislation. Through partnerships with the Office of the Chief Procurement Officer (OCPO), OCIO, and divisions of the Office of the Chief Financial Officer (OCFO), including the Division of Financial Assistance Policy and Oversight (FAPO), DHS established several working groups. The working groups are the Headquarters DATA Act Working Group, the Component Implementation Working Group, the Technical Solution Team, and the Financial Assistance Sub-Team.

The DATA Act Project Team communicated early and often with these groups, and continues to do so as DHS navigates its day-to-day implementation of the act. It is this ongoing, frequent, and transparent communication that has helped DHS successfully secure buy-in from the various stakeholders represented by its working groups. Outside of working group meetings, members have access to DATA Act-specific SharePoint sites that allow members to work on their individual needs as well as foster group communication and collaboration.

Key accomplishments include the establishment of a central DHS DATA Act Enterprise Repository, and the submittal of a modified Implementation Plan Update and costing estimates to OMB/Treasury with substantial input from all DHS Components. Key upcoming milestones include achieving the ability to receive first FY 2017 data supplier transmission by January 2017, and provide agency data to Treasury in DATA Act schema format by FY 2017.

USAspending.gov

The Department's OCFO will continue to assess quarterly the accuracy, completeness, and timeliness of data posted to USAspending.gov, the main portal for financial data on government contracts and financial assistance awards.

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

Milestones to support the accuracy, completeness and timeliness of all financial assistance data posted to any public venue	**Finish Date**
Develop standard model for reporting /New Access Reporting Tool/Exception Reports on posted USAspending data	Completed April 2014:

Provide oversight of USAspending.gov data with monthly exception and comparison reports. Corrections and missing data posted as a result of	Recurring
Bring DHS closer to compliance with FFATA and Data Act requirements.	In Process
Develop business models and business rules related to reporting for the DHS-wide enterprise system.	In Process

Table 1 – Data Integrity Milestones

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

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

VII. Ongoing Initiatives at DHS

Participation in Transparency Initiatives

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

Data.gov

DHS is committed to safeguarding sensitive information while promoting a culture of information sharing and considering all high value data for release to the general public and interested developers, to state, local, tribal, and federal partners, to university and research programs, and to other DHS Components and programs.

E-Rulemaking

Federal regulations have been available for public comment for many years, but historically users needed to visit a government reading room to provide comments. Today, under the E-Rulemaking process, the American public can share opinions from anywhere with an available Internet connection via Regulations.gov website.

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

IT Dashboard

In support of promoting transparency, DHS is currently reporting information on 92 major IT investments to the IT Dashboard. The IT Dashboard is a website enabling federal agencies, industry, the general public, and other stakeholders to view details of federal information technology investments.

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

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

CFDA.gov

The Catalog of Federal Domestic Assistance (CFDA) is a government-wide compendium of federal programs, projects, services, and activities that provide assistance or benefits to the American public. It contains financial and nonfinancial assistance programs administered by departments and establishments of the federal government. Currently, DHS has 73 programs listed in the CFDA.

Grants.gov

Grants.gov provides a single website to find and apply for federal discretionary grants. Grants.gov provides over one million organizations a single web site where they can find and apply for over $500 billion worth of grants distributed annually.

In FY 2015, DHS posted Notice of Funding Opportunity Announcements representing over 60 programs on Grants.gov. These opportunities resulted in approximately 7,800 awards to a total of about 4,800 grant recipients totaling approximately $10 billion.

Websites

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

- Digital Strategy Website: https://www.dhs.gov/dhs-digital-strategy
- DHS.gov Website Metrics: https://www.dhs.gov/publication/dhsgov-web-performance-metrics-2016
- Examples of commonly sought-after information:
  - "Check Immigration Case Status"
  - "Careers"
  - "Trusted Traveler Programs"

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

Whistleblower Protection

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

Protecting Employees with Access to Classified Materials

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

- The Personnel Security Division within the Office of the Chief Security Officer coordinated efforts with the Office of General Council to develop a revised Notice of Determination letter template including PPD-19 language for use throughout the Department. This template was distributed to Components in September 2013.
- The Personnel Security Division updated the DHS Instruction 121-01-007 "Personnel Security and Suitability Program" to include PPD-19 language and procedure. This Instruction provides Department policy and guidance to headquarter and operational Component personnel security offices. The revised document was issued on June 11, 2015.

Protecting Employees

The Department provides information to employees about their rights as a whistleblower in a decentralized manner. To ensure that the information provided is current and consistent with best practices, the Office of Special Counsel Certification and has taken the following steps:

- Established an intranet site that shares information from the Office of Special Counsel (OSC) on whistleblower protections and other areas under their jurisdiction.
- Distributed and posted OSC promotional materials in all DHS locations.
- Provided the annual reminder to employees and supervisors on their roles and rights under Whistleblower, required training and referred them to the new website.
- Required all supervisors to take the Prohibited Personnel Practice/Whistleblower Disclosure Training Quiz as required by OSC.
- Designated a Whistleblower Ombudsman in the Office of Inspector General (OIG).
- Began drafting a directive codifying requirements and establishing responsibilities.

DHS applied for OSC certification on April 25, 2016.

Public Notice

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

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

The Department publishes a Federal Register Notice for the following:

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

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

Records Management

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

The Department's Records Management program office and Component records programs continue to collaborate with the legal and FOIA lines of business to build stronger information Governance processes and policies across the enterprise. The Department has established working groups and advisory teams to ensure that mission needs, memorandum objectives and functional system requirements are incorporated into a potential solution. The Department is exploring options for implementing an eDiscovery and Electronic Records Management System. An integrated, enterprise-wide system will enable the Department to automate many currently manual processes, provide the technology to manage all electronic records in their native format and ensure compliance with requirements outlined in the 2012 Managing Government Records Directive.

The Department continues to make information available on the status and progress of its initiatives, by distributing information through the records management governing body, the Records Leadership Council (RLC), and by publicizing information on its intranet web presence. This ensures that all DHS employees have access to updates and current status.

The Department provides updates and is accountable to the designated Senior Agency Official (SAO), who is responsible for all of the records management objectives to the Archivist of the United States (AOTUS).

To ensure the objectives are met, the SAO has instituted email journaling, a process in which all electronic email messages are captured while still in transit, and preserved in their native electronic format. The process ensures that all email messages, whether permanent or temporary in record value, are captured and preserved, and is not dependent on user interaction.

Congressional Requests

The Department values communications with Congress as a central tenet of its open government efforts. The Office of Legislative Affairs provides briefings, testimony, background information, staff

discussions and field visits for Congressional members for a better understanding of DHS operations. OLA communicates accurate and detailed information to congressional interests, while following appropriate protocols to safeguard classified or otherwise sensitive information.
For additional information, please visit http://www.dhs.gov/about-office-legislative-affairs.

Declassification of Department of Homeland Security Information

Pursuant to Executive Order (EO) 13526, DHS routinely reviews information to affirm classification and to declassify when possible. DHS is also undertaking a fundamental review of all classification and declassification guides. The reviews will evaluate 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 EO 13526. DHS intends to have its declassification guides resubmitted to the Interagency Security Classification Appeals Panel for approval by December 2016, and to have updated its classification guides by June 2017.

In 2016, the DHS OIG began a follow-up to its 2013 review, *Reducing Over-Classification of DHS' National Security Information*, which reviewed the classification program at large at DHS. The original 2013 report may be accessed at: http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-106_Jul13.pdf.

Emphasis on Plain Writing

DHS understands that plain writing is vital for achieving the goals of Open Government. According to the Plain Writing Act of 2010, plain writing is, "writing that is clear, concise, well-organized, and consistent with other best practices appropriate to the subject or field and intended audience. Such writing avoids jargon, redundancy, ambiguity, and obscurity." DHS values public comments and welcomes feedback about how we provide all internal and external stakeholders with documents and materials that are clearly written.

Federal Plain Language Report Card – 2015, Prepared by the Center for Plain Language, issued DHS an "A+" rating for Compliance with the Plain Writing Act of 2010, and an "A" rating for Writing and Information Design.