DoD Open Government Plan Version 3.0

June 1, 2014

Section I - Introduction

Background

On January 21, 2009, shortly after assuming office, the President of the United States issued the Presidential Memorandum on Transparency and Open Government, setting forth three basic principles for agencies of the executive branch to pursue as the normal course of business: transparency, participation, and collaboration.

On December 5, 2013, the second Open Government National Action Plan (NAP 2.0) was released by the White House building upon the first National Action Plan which was released on December 8, 2009. NAP 2.0 continues the main points of the original and adds new requirements such as Proactive Disclosure and Whistleblower Protection.

Department of Defense Involvement in Open Government Activities

It surprises many to learn that the Department of Defense has led the way in transparency for decades. No other agency has broadcasting studios for major news organizations in its headquarters building. Most people have seen news correspondents embedded with combat units reporting from "somewhere in" the war zone as well as the Secretary of Defense and the Chairman of the Joint Chiefs of Staff sharing a briefing podium on a regular basis.

The Department's work to further the President's vision began in early 2009 as data.gov was developed and launched and has grown continually, in parallel to efforts of the Federal Government as a whole. What began as an informal partnership between the Office of the Assistant Secretary of Defense (Public Affairs) and Office of the Assistant Secretary of Defense (Networks & Information Integration)/DoD Chief Information Officer has led, upon issuance of the Open Government Directive, to a governance structure under the leadership of the Office of the Deputy Chief Management Officer, as designated by the Deputy Secretary of Defense.

Senior Accountable Officials at DoD

In December 2009, upon issuance of the Open Government Directive (OGD), the Deputy Secretary of Defense designated the Deputy Chief Management Officer (DCMO) as the senior accountable official for the Department's implementation of Open Government efforts and is responsible for the Department's overall Open Government strategy and execution. The Assistant Deputy Chief Management Officer maintains day-to-day oversight of the Open Government initiative to assure that the principles of the OGD are adhered to as we implement and refine our Open Government Plan.

Mr. Michael J. McCord, Principal Deputy Under Secretary of Defense (Comptroller), is designated as the senior official accountable for the quality and objectivity of, and internal controls over, federal spending data disseminated by the Department to the public.

A Living Document

This plan is by its nature unfinished and is intended to be a living document. It is not all-inclusive and should be used in conjunction with the Department's Open Government website [http://www.defense.gov/open] which will have the latest information and links to more detailed information.

Section II – New and Expanded Initiatives

Open Data

For the latest information, click on
http://data.defense.gov/

Data.gov

Since the launch of Data.gov [*http://www.data.gov*] in May 2009, DoD has been committed to expanding public access to information and adopting a presumption in favor of openness and access. The Department will continue to use Data.gov as the access point for an ever increasing quantity of high-value, authoritative data that is not restricted for national security, privacy or other statutory reasons.

M-13-13, Open Data Policy – Managing Information as an Asset

On May 9, 2013, the White House released M-13-13 which requires agencies to collect or create information using machine-readable and open formats, data standards, common core, and extensible metadata for all new efforts.

The Department is in the process of systematically inventorying its data assets and evaluating which datasets can be released to the public. In the near term, this is being done through the existing data.gov dataset workflow process. The long-term solution will be to manage this through the Defense Information Technology Portfolio Repository (DITPR) system.

The Department is also making data available to internal components, other agencies, and the public through a diverse set of Web Application Programming Interfaces (APIs). A listing of those approved for public use is available at *http://www.defense.gov/developer*.

Many of the common examples of the value of open data are actually Department of Defense data assets. For example, the Global Positioning System (GPS) is a space-based satellite navigation system built and maintained by DoD and is freely available to anyone in the world with a GPS receiver. In addition to navigation, uses of GPS include precise timing for financial transactions, search and rescue, communications, farming, recreation and both military and commercial aviation. GPS is operated by the 2nd Space Operations Squadron at Schriever Air Force Base, Colorado.

Another example is weather data. The National Weather Service was originally known as the Weather Bureau of the United States under the Secretary of War as Congress felt that "military discipline would probably secure the greatest promptness, regularity, and accuracy in the required observations." While under the Secretary of War, it was part of the US Army Signal Corps. In modern times, DoD developed and launched the first weather satellite, Vanguard 2, on February 17, 1959 as part of the US Navy's Operation Vanguard and now operates the Defense Meteorological Satellite Program which are the most sophisticated weather satellites in the world. DoD also makes major contributions to global weather forcasting through the US Air Force Weather Agency and the Naval Meteorology and Oceanography Command.

While the Department has a tremendous amount of data that it releases for public consumption, much of our data cannot be released in real-time due to national security considerations. Requests for specific information or for the release of a general type of information through data.gov can be made on our Open Data website feedback page located at *http://data.defense.gov/ContactUs.aspx*.

Proactive Disclosure

For the latest information, click on
http://open.defense.gov/ProactiveDisclosure.aspx

The Office of the Secretary of Defense and the Joint Staff (OSD/JS), the Department of the Air Force, and the Armed Services Board of Contract Appeals (ASBCA) are examples of Department of Defense Freedom of Information Act (FOIA) components taking steps to proactively disclose information highly sought-after by the public. The OSD/JS and the Department of the Air Force implemented procedures whereby all document releases to the public made under the FOIA are proactively posted to their FOIA libraries, except for those releases that contain privacy concerns. Additionally, the OSD/JS recently began a proactive disclosure initiative that posts, within the FOIA library, document releases made in response to Mandatory Disclosure Review requests.

The ASBCA is a neutral, independent forum with the primary function of hearing and deciding post-award contract disputes between government contractors and the Department of Defense; the National Aeronautics and Space Administration; the Central Intelligence Agency, as appropriate; and other entities with whom the ASBCA has entered into agreements to provide services. The ASBCA functions under the Contract Disputes Act (41 U.S.C. §§ 7101-7109), its Charter, or other remedy-granting provisions. The majority of matters on the ASBCA's docket involve appeals by contractors from government contracting officers' final decisions or failures to issue decisions. Because of the high public interest in its decisions, ABSCA is now posting all decisions and dismissal orders related to matters on its docket. Previously, ASBCA only posted decisions or dismissal orders that contained significant legal analysis likely to be of interest to government contracts law practitioners.

Privacy

For the latest information, click on
http://open.defense.gov/Transparency/PrivacyActandRecords.aspx

The Defense Privacy and Civil Liberties Office

The mission of the Defense Privacy and Civil Liberties Office (DPCLO) is to implement the Department of Defense's Privacy and Civil Liberties programs through advice, monitoring, official reporting and training. Various privacy compliance reports produced by DPCLO and other DoD offices include:

System of Records Notices (SORNs)

A system of records is a group of records, in any storage media (paper, electronic, etc.), under the control of a DoD component from which personal information about an individual is retrieved by the name of the individual, or by some other identifying number, symbol, or other identifying particular assigned, that is unique to the individual. The DoD publishes in the *Federal Register* a system of records notice (SORN) for all systems of records maintained on individuals associated with DoD. The public can also access these notices on the DPCLO web page: *http://dpclo.defense.gov/Privacy/SORNs.aspx*.

The Senior Agency Official for Privacy (SAOP) portion of DoD's annual Federal Information Security Management Act (FISMA) Report

DoD's annual FISMA report includes input from the SAOP, the Office of the Chief Information Officer (CIO) and the Inspector General. The CIO compiles the report and submits it to the Office of Management and Budget (OMB) and the Government Accountability Office. DoD's annual FISMA report is not made available to the public. However, OMB provides Congress with an annual summary on Federal agencies' FISMA implementation. The most recent OMB summary report is available on the OMB Office of E-Government and Information Technology web page. OMB provides a summary of *http://www.whitehouse.gov/omb/e-gov/docs*.

Quarterly Section 803 Reports

Section 803 of Public Law 110-53, "Implementing Recommendations of the 9/11 Commission Act of 2007," requires DoD to submit periodically, but not less than quarterly, a Privacy and Civil Liberties Report to Congress and the Privacy and Civil Liberties Oversight Board. The public can access these reports on the DPCLO web page: *http://dpclo.defense.gov/Privacy/Resources/Reports.aspx*.

Biennial Computer Matching Activity Report

Computer matching is a computerized comparison of two or more Federal automated systems of records, or between a Federal system of records and non-Federal records, to establish or verify eligibility or compliance regarding Federal benefit programs. DoD's biennial computer matching activity report is submitted to OMB and to Congress. The public can access these reports on the DPCLO web page: *http://dpclo.defense.gov/Privacy/Resources/Reports.aspx*

Privacy Impact Assessments

DoD recognizes that the protection of personal information is important throughout the life cycle of the information. The vehicle for addressing privacy issues in an information system or electronic collection is the DD Form 2930, Privacy Impact Assessment (PIA). DoD requires the completion of a PIA when developing or procuring information systems or electronic collections that collect, maintain, use or disseminate personal information on the general public, Federal personnel, contractors, and foreign nationals employed at U.S. military facilities internationally. The goal of the PIA process is to identify privacy risks and privacy protections that will be integrated during the development life cycle of the information system or electronic collection. The public can access these reports on the CIO's web page: *http://dodcio.defense.gov/Home/Issuances/DoDCIOPrivacyImpactAssessments(PIAs)/DoDComponentPrivacyImpactAssessments.aspx*.

Whistleblower Protection

For the latest information, click on
http://www.dodig.mil/programs/whistleblower/index.html

The Department of Defense was certified by the U.S. Office of Special Counsel as having completed the 2302(c) Whistleblower Act Certification Program [http://www.osc.gov/outreachAgenciesCertified.htm] on June 10, 2012.

The Department's investigators, auditors, evaluators, and inspectors rely on whistleblowers to provide information as a source of allegations and as original and corroborating evidence. Federal employees within the Executive Branch are required to report corruption. When they do so through the Inspector General Act of 1978, the DoD Inspector General (IG) can investigate alleged reprisal against those whistleblowers. Whistleblowing is not a 'nice to have' function; it is essential to the national security and defense mission of the Federal government.

Employees must take No Fear training at least biannually, which includes information on Whistleblower protection including their individual rights and how to submit a Whistleblower Protection complaint.

Additionally, the National Defense Authorization Act for Fiscal Year 2013 extended these protections to contractor employees of DoD effective on July 1, 2013. The expanded protection applies to employees of both prime contractors and subcontractors. The type of information protected has also expanded to include disclosures of:

- Abuse of authority in the management of a DoD contract or grant
- Violations of rules and regulations related to a DoD contract
- Initiation of or participation in any judicial or administrative proceeding related to waste, fraud or abuse on a Department of Defense contract or grant

To assist potential whistleblowers, the Inspector General has designated a Whistleblower Protection Ombudsman (WPO) for the Department of Defense. The WPO is available to assist civilian employees, military members, and contractors as well as members of the Defense intelligence community seeking protection under the Defense Intelligence Community Whistleblower Program (DICWP).

Websites

For the latest information, click on
http://open.defense.gov/portals/23/Documents/DoD_Customer_Service_Plan.docx

The Department is committed to consistently providing a quality customer experience through the continuous improvement of customer service delivery across many diverse lines of business and services. This commitment was recently reinforced by the President's Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service," April 27, 2011, and

Office of Management and Budget Memorandum M-11-24, "Implementing Executive Order 13571 on Streamlining Service Delivery and Improving Customer Service," June 13, 2011, requiring Federal agencies to develop customer service plans. The goal of customer service in DoD is to ensure customers receive increasingly better service, through the real-time adoption of process improvements and supporting technologies that focus on timeliness, accuracy, and responsiveness.

Continuous improvement of customer service across the DoD is supported by a large set of policies and specific activities, which include ensuring the accessibility of information and services to Americans with disabilities; automating work flows; ensuring discovery through centralized and federated search; improving confidentiality, integrity and authenticity of information; and across the board compliance with laws and Federal regulations.

The public website of *www.defense.gov* provides viewers with a knowledge base to address a variety of subjects related to the Department of Defense and the Military services, and a feedback mechanism for the viewer to submit any unique questions or concerns that are not addressed in the FAQ section. Web usability guidance by a partnership between U.S. Department of Health and Human Services and the U.S. General Services Administration through the public website of www.usability.gov helps provide DoD web presences with best practices for usability and ease of navigation. The search feature for www.defense.gov provides a very feature-rich search service for viewers that is supported by the DigitalGov search service provided by the U.S. General Services Administration.

An analysis of the Department's Web usability can be found at:
http://open.defense.gov/portals/23/Documents/DoD_Customer_Service_Plan.docx

Section III – Ongoing Initiatives

Participation in Transparency Initiatives

For the latest information, click on
http://open.defense.gov/Transparency.aspx

DoD has taken numerous steps to foster greater public participation in the Department's ongoing efforts to increase transparency, participation, and collaboration. While the Internet has been a main pathway of communication to the public for many years, it is now being used to interact with and gain input from the public through Web 2.0 technologies. The techniques and methods that DoD uses to engage with the service members and the public described in the following sections.

DoD Blogging

Daily updates from Pentagon Channel reporters, Bloggers Roundtable speakers are available at http://www.dodlive.mil/index.php/category/bloggers-roundtable/. Senior Defense Department officials on DoD news and information, Pentagon Channel programming, pertinent DoD coverage by mainstream media, and other DoD media are posted at http://www.dodlive.mil/.

Microblogging

The Department uses microblogging platforms [http://www.defense.gov/releases/](i.e. Flickr, Twitter, Facebook, and YouTube) to not only push out useful information, but also as a means to engage in a two-way dialogue with the public.

Social Media Directory

The Department's social media directory lists all of DoD's official pages across various social media networks.

- Defense Department - http://www.defense.gov/RegisteredSites/SocialMediaSites.aspx
- Army - http://www.army.mil/media/socialmedia/
- Navy - http://www.navy.mil/socialmedia/
- Marines - http://www.usmc.mil/usmc/Pages/SocialMedia.aspx
- Air Force - http://www.af.mil/socialmedia.asp

Daily Online News Updates

Press advisories, releases, transcripts, announcements of upcoming key events and daily overviews are regularly updated at http://www.defense.gov/news/news.aspx.

Online Videos

Video of briefings, speeches, interviews and presentations by the Department's senior leadership are routinely made available and archived on the Pentagon Channel's website at http://www.pentagonchannel.mil/.

Public Notice

For the latest information, click on
http://open.defense.gov/Transparency/ElectronicRulemaking.aspx

There are many existing programs and Internet presences you can use to learn more about the Department of Defense, its leadership and operation, and to connect with service members. Here are but a few:

Senior Leadership Travel

Travel by Secretary Hagel and other senior leaders is regularly highlighted at http://www.defense.gov/home/features/travels/.

Community Relations Programs

The Community Relations website at http://www.ourmilitary.mil/ provides resources for connecting with troops.

Capitol Hill Hearings

The Office of the Assistant Secretary of Defense (Legislative Affairs) maintains a public calendar of Department officials testifying on Capitol Hill at http://la.defense.gov/.

Joint Civilian Orientation Conference

The Joint Civilian Orientation Conference (JCOC) [http://jcoc.dod.mil/] is a program sponsored by the Secretary of Defense for civilian public opinion leaders interested in expanding their knowledge of military and national defense issues. JCOC is the oldest existing Pentagon outreach program, having been held more than 76 times since 1948.

Employer Support of the Guard and Reserve

Employer Support of the Guard and Reserve (ESGR) [http://www.esgr.mil] is a staff group within the Office of the Assistant Secretary of Defense for Reserve Affairs which seeks to promote a culture in which all American employers support and value the employment and military service of members of the National Guard and Reserve. ESGR, with committees in all 50 states and territories staffed by over 4,800 volunteers, facilitates and promotes a cooperative culture of employer support for National Guard and Reserve service by developing and advocating mutually beneficial initiatives; recognizing outstanding employer support; increasing awareness of applicable laws and policies; resolving potential conflicts between employers and their service members; and acting as the employers' principal advocate within DoD. ESGR also promotes several important programs including the Hero2Hired program [https://h2h.jobs], and the "Bosslift" program which provides employers an opportunity to visit military installations, go aboard a ship and/or ride on military aircraft to observe National Guard and Reserve members on duty and see firsthand the quality of training and leadership activities their uniformed employees receive as part of the total force.

Ceremonial and Patriotic Events

Military color guards, musical units, aviation units and other organizations provide public performances at well over 10,000 events a year across the nation, including patriotic openers to public events, flyovers, concerts and static displays of military hardware.

Tours of the Pentagon and Beyond

The Pentagon Tours program [http://pentagon.osd.mil/tour-selection.html] annually brings over 100,000 visitors to the Department's headquarters. Various commands, installations and ships also hold programs allowing the public to more closely connect with the Department and its personnel. Please note that tours must be scheduled in advance.

Public Queries

The Office of the Secretary of Defense's Public Communications Office annually responds to over 30,000 comments and requests for information from the general public.

Records Management

For the latest information, click on
https://intellipedia.intelink.gov/wiki/DoD_Records_Management

The Department issues policy guidance and works with the National Archives and Records Administration (NARA) to ensure valuable records are carefully maintained for future use.

DoD Compliance With Existing Records Management Requirements

The Department's primary policy directive, DoD Directive 5015.02 (http://www.dtic.mil/shs/directives/corres/pdf/501502p.pdf) provides overarching records management guidance for all Department Components. In turn, Components have their own subordinate policy documents which locally implement the Department-wide issuance. Subordinate commands and organizations may have even more specific published guidance. Each of these is compliant with policy and regulations from NARA.

- The Department of the Army's Records Management and Declassification Activity can be found at https://www.rmda.army.mil/.

- The Department of the Navy's records management program can be found at http://www.doncio.navy.mil/PolicyView.aspx?ID=707.

- The Department of the Air Force's key documents for records management include AFI 33-321, Authentication of Air Force Records, AFI 33-322, Records Management Program, AFMAN 33-363, Management of Records, and AFI 33-364, Records Disposition, Procedures and Responsibilities. They are all available at http://www.e-publishing.af.mil/.

- In the case of Combatant Commands (which are responsible for either a geographic area (e.g., U.S. Pacific Command) or a functional area (e.g., U.S. Transportation Command), the Office of the Chairman of the Joint Chief of Staff provides records management guidance through the Chairman of the Joint Chiefs of Staff Instruction 5760.01A, available at http://www.dtic.mil/cjcs_directives/cdata/unlimit/5760_01.pdf.

- Additional guidance for The Office of the Secretary of Defense, Defense Security Cooperation Agency, Defense Advanced Research Projects Agency and Certain Field Activities is provided by Administrative Instruction 15, available at http://www.dtic.mil/whs/directives/corres/ins2.html. The website at http://www.dtic.mil/whs/esd/rdd/recordsmgt.html provides additional materials and links.

The Managing Government Records Directive (MGRD) Senior Agency Official (SAO) Annual Report

The annual MGRD SAO report documents the Department's progress towards the successful implementation of the OMB/NARA Managing Government Records Directive (M-12-18), as well as provides insight into key Component/Independent Agency records management issues and critical milestones related to long-term initiatives. The DoD CIO compiles the report based on input from all Components/Independent Agencies, and submits it to NARA. The most recent report is available on the DoD Records Management wiki page at *https://intellipedia.intelink.gov/wiki/DoD_Records_Management*.

Freedom of Information Act (FOIA) Requests

For the latest information, click on
http://open.defense.gov/Transparency/FOIA.aspx

Overall Structure

The FOIA Program at the Department operates under the authority of the DoD Chief FOIA Officer, Mr. Michael L. Rhodes, Director of Administration and Management (DA&M), Office of the Secretary of Defense. This senior official is responsible for monitoring FOIA implementation for the Department and ensuring compliance with governing FOIA policies and procedures in accordance with the FOIA, 5 U.S.C. 552. Additionally, the Defense Freedom of Information Policy Office (DFOIPO) [*http://www.dod.mil/pubs/foi/dfoipo/*] is responsible for the formulation and implementation of FOIA Policy for the Department on behalf of the Director of Administration and Management. Due to its size and complexity, the DoD FOIA Program is decentralized, with operations at hundreds of FOIA offices worldwide. Each DoD Component operates its own FOIA office and responds to FOIA requests for its own records.

FOIA Requestor Service Centers

The DoD FOIA Requester Service Centers are the initial starting point for requesters to submit a FOIA request and receive additional information pertaining to the status of a pending FOIA request. The DFOIPO website, available at *http://www.dod.mil/pubs/foi/dfoipo/*, provides links to the DoD FOIA Requester Service Centers and a listing of FOIA Public Liaisons [*http://www.dod.mil/pubs/foi/dfoipo/docs/FOIA_RequesterServiceCenterContacts.pdf*], should you need customer service regarding a FOIA request. The FOIA Public Liaisons report to the agency Chief FOIA Officer and serve as the supervisory official to whom a requester can raise concerns, following an initial response from the FOIA Requester Service Center. FOIA Public Liaisons also assist in reducing FOIA delays, providing the status of FOIA requests and assisting in the resolution of disputes. For maximum efficiency in initiating a DoD FOIA request or to learn more about the DoD FOIA Program, interested parties should reference the DoD Freedom of Information Handbook [*http://www.dod.mil/pubs/foi/dfoipo/foiaHandbook.html*].

When a FOIA Requester Service Center receives a FOIA request, the request is first analyzed to determine whether or not it conforms to FOIA and Agency regulations. Next, each Requester Service Center determines the staff office within the component that would most likely have responsive documents, and tasks that specific office to find and review the responsive

documents. Once reviews are complete, a response is sent to the requester with any number of possible answers. The response could provide the requester with one or more of the following: all documents requested; documents requested with some information redacted; a denial of documents in their entirety; an explanation that the requested documents were not located; or an explanation that the documents were sent to another agency or department component for review.

Electronic FOIA Reading Rooms

FOIA amendments signed into law in 1994 added a requirement that agencies must establish an Electronic FOIA (EFOIA) Reading Room. The EFOIA Reading Room contains such materials as certain DoD manuals, specific DoD policy statements, and opinions developed in the adjudication of cases. At the Department, each DoD Component, to include the Military Services, Department of Defense Agencies, and Combatant Commands maintains its own Reading Room.

- Military Services: [*http://www.dod.mil/pubs/foi/dfoipo/mil_services.html*],
- Department of Defense Agencies [*http://www.dod.mil/pubs/foi/dfoipo/def_agencies.html*],
- Combatant Commands [*http://www.dod.mil/pubs/foi/dfoipo/combatant_command.html*],

On our Open Government website, we've also added links to the major FOIA Reading Rooms maintained across the Department, which contain frequently requested material and are regularly updated.

Backlog Reduction

Overall, the Department is improving its capacity to analyze, coordinate, and respond to requests in a timely manner. In 2008, the Department updated its FOIA backlog reduction plan that gave DoD Components guidance on how to target their individual FOIA backlogs. When the plan was implemented, the FOIA backlog at the end of FY 2008 was 11,571 requests. A 10% reduction per year extrapolated over the next five years (FY 2009-2013) would result in 6832 backlogged cases. As was reported in the DoD FOIA Program Annual Report for FY 2013, the backlog was actually reduced to 6593 requests, exceeding the 10% per year goal by 239 requests.

The Department recognizes that sustaining this success will be difficult given current fiscal restraints that have resulted in a reduction of available resources. However, DoD Components continue to engage their senior leadership in focusing on implementing new ways to reduce FOIA backlogs by continuing to implement the procedures outlined in the previous plan. One of the primary methods in reducing backlogs is through the use of new information technology tools. Several years ago the Department of Defense was the leading government agency in implementing ways to transfer documents electronically from one FOIA office to another, at any classification level, instantaneously. These tools, which are now common business practices among agencies, have proven to save both time and resources in the processing of documents responsive to FOIA requests, while providing a more secure method of transfer than using the mail, courier services, or even emails. Additionally, many DoD Components have concentrated available resources on closing its oldest FOIA requests.

A major aspect of reducing FOIA backlog is having a robust FOIA training program. Due to resource restraints within the past two years, the DoD has shifted its major emphasis of training to online training through Defense Connect Online (DCO) medium. The Defense Freedom of Information Policy Office (DFOIPO) utilizes DCO in two ways; first, online training is provided on the administrative/procedural issues (to include the President's and Attorney General's FOIA policies) and on the FOIA exemptions in a real time format that allows the participants around the world to ask questions of the presenter and engage in informative discussions with other participants. These training sessions are recorded for future use. Second, DFOIPO regularly holds "FOIA Chat" sessions where one or more experienced FOIA experts are available for purposes, such as discussing issues relevant to the DoD FOIA community new case law, or answering questions online from other participants. Experience shows that these online FOIA Chats assist DoD FOIA officers and attorney by providing tools to facilitate the processing of FOIA requests, explaining and clarifying case law and FOIA policy guidance, and encouraging the sharing of best practices among the participants. When the Department of Justice online FOIA training modules become available soon, it is envisioned that these models will render the current DCO training sessions obsolete; however, the FOIA Chat sessions will continue.

As resources become available again for training and travel, DFOIPO is revisiting the plan implemented several years ago of conducting FOIA training workshops at geographical locations having a concentration of DoD personnel and available no-cost training facilities. In past years these workshops proved to save significant resources by bringing the instructors directly to the personnel needing the training. As the Department of Justice training modules come online, DFOIPO plans to have available for the DoD a mix of online training, in-person training, and ongoing "FOIA Chat" discussions via DCO that will be aimed to providing the FOIA officer the tools necessary in reducing FOIA backlogs.

Congressional Requests

For the latest information, click on
http://open.defense.gov/Transparency/CongressionalInquiries.aspx

The Office of the Assistant Secretary of Defense for Legislative Affairs is responsible for coordinating all requests for information from Congress including senior officials testifying at hearings. The homepage can be found at *http://la.defense.gov/*, and includes a general description of how the office functions and administers legislative affairs for the Department with Congress and the White House. The office is continuing to improve the website within the bounds of the Department's security regulations. Key documents describing the Department's processes for handling congressional requests for information include:

- Department of Defense Directive 5142.01, "Assistant Secretary of Defense for Legislative Affairs (ASD(LA))," available at *http://www.dtic.mil/whs/directives/corres/pdf/514201p.pdf*.

- Department of Defense Instruction 5400.04, "Provision of Information to Congress," available at *http://www.dtic.mil/whs/directives/corres/pdf/540004p.pdf*.

- Department of Defense Instruction 5545.02, "DoD Policy for Congressional Authorization and Appropriations Reporting Requirements," available at http://www.dtic.mil/whs/directives/corres/ pdf/554502p.pdf.

Declassification

For the latest information, click on
http://open.defense.gov/Transparency/Declassification.aspx

In December 2009, President Obama issued an Executive Order to increase the speed and efficiency of declassifying over 400 million pages of historical records across the government, many of which involve DoD are of interest to academia, the media and the public at large.

Structure

The Department is the single largest declassifying organization (in terms of number of pages released) in the Federal government. Each one of the Department's Components maintains its own program to meet declassification timelines for executing automatic and mandatory declassification reviews delineated in President Obama's December 2009 Executive Order 13526, "Classified National Security Information" (document available at http://edocket.access.gpo.gov/2010/pdf/E9-31418.pdf). The Department adopts a framework of centralized oversight with decentralized execution of declassification activities across the Department. This allows for a risk-based approach to balancing the imperatives of public transparency and protection of national security.

National Declassification Center

To facilitate declassification, the Department strongly supports the National Declassification Center created by the President's Executive Order. The Department provides business process reengineering expertise to the National Archives and Records Administration who, along with a team of experts from across the federal government, are dedicated to the retirement and release to the public of over 400 million pages of records now held in the College Park, Maryland facility. Likewise, these efforts will serve to modernize the overall declassification system. The Department will continue to work with the National Archives and Records Administration to ensure information regarding activities of the new National Declassification Center is made available through appropriate Web-enabled environments to include Data.gov. More information on the Center can be found at http://www.archives.gov/declassification/.

Department of Defense Joint Referral Center

To jumpstart our involvement with the National Declassification Center, the Department established a Joint Referral Center. This element serves as an adjunct to the National Declassification Center where Department of Defense Components may jointly pilot new business processes and technologies to streamline and standardize how we manage referrals in the declassification process.

Our declassification approach includes:

- Supporting structured reviews within the business process reengineering effort to standardize declassification processes and ensure they are optimized for future operations;

- Establishing a capability for prioritizing information that is informed by the National Archives and Records Administration outreach to, and interface with, the public interest declassification community and the American people;

- Establishing the Department of Defense Joint Referral Center, to ensure a central mechanism for rapid coordination across all Department Components to clear permanently valuable records slated for declassification;

- Collaborating closely with the National Archives and Records Administration on their National Declassification Center Strategic Communications campaign, including providing essential content and articles for their website; and

- Publishing an expedited update during calendar year 2010 to key Department regulations (DoDI 5200.01, "*DoD Information Security Program and Protection of Sensitive Compartmented Information*," and DoD 5200.1-R, "*Information Security Program*"), which implement requirements of President Obama's December 2009 Executive Order[1].

Initiating a Declassification Review

The key document and other supporting reports describing the Department's process for handling declassification of DoD records include:

- DoD Manual 5230.30-M, "DoD Mandatory Declassification Review (MDR) Program, "December 12, 2011, available at *http://www.dtic.mil/whs/directives/corres/pdf/523030m.pdf*.

- National Declassification Center Prioritization Plan, available at: *http://www.archives.gov/declassification/final-prioritization-plan.pdf*.

- Biannual Report on Operations of the National Declassification Center, available at: *http://www.archives.gov/declassification/reports/2010-biannual-january1-june30.pdf*.

Collaboration

For the latest information, click on
http://open.defense.gov/Transparency/Collaboration.aspx

Organizations in the Department of Defense community use a variety of collaboration platforms and tools including:

Intelink

The Intelink platform provides access to authorized users across the Department and other Agencies to SharePoint collaboration tools, instant messaging and Intelipedia, a wiki-based collaboration and information sharing tool.

[1] The current version is available at *http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf*

Defense Connect Online
The Defense Connect Online tool provides Web conferencing (to include audio, video, chat, instant messaging, screen sharing, etc.) and chat capabilities for users across the Department enterprise. Defense Connect Online is composed of two commercial tools and a custom portal for access. Adobe Connect is the Web conferencing application and Jabber is the Extensible Messaging and Presence Protocol (XMPP) secure chat service and client.

Service and Command Centric Platforms
Each of the Military Services maintains a variety of collaboration platforms and tools specific to their particular needs and operations. These include Defense Knowledge Online, Army Knowledge Online, Navy Knowledge Online, MarineNet, and Air Force Knowledge.

Section IV - Flagship Initiatives

Declassification of Formerly Restricted Data

For the latest information, click on
http://open.defense.gov/Transparency/FRDDeclass.aspx

Formerly Restricted Data (FRD) is classified information jointly determined by Department of Energy (DoE) and DoD to be related primarily to the military utilization of nuclear weapons and removed from the Restricted Data category (and remains protected as classified FRD information) pursuant to the Atomic Energy Act, as amended.

The Second Open Government National Action Plan for the United States of America (NAP 2.0) called for the DoD, DoE, and Department of State (DoS) to determine, consistent with applicable statutes, how to implement a systematic review process for the declassification of no-longer sensitive historical FRD information on nuclear programs focusing on specific events and topics of historical nuclear policy interest and ways for the public to help identify priorities for declassification review.

DoD and DoE have developed a process to begin the declassification process with DoS participating as necessary. Under the Joint DoD-DoE working process, FRD topics are brought forward thru routine partnership and engagement and are evaluated for declassification in the context of technical, policy, political, and administrative benefits.

- Example: 2010 Stockpile declassification decision;
- Example: decisions leading to routine updates to nuclear weapons security classification guides by DoE.

Our joint FRD declassification process is systematic, but it is important to note that it has no relationship to the Executive Office (EO) 13526, Section 3.4 [systematic] processes or requirements. As our process continues to mature, we will also be evaluating for declassification FRD topics that are highly "tabbed" (marked as possibly containing FRD) during United States Government Department and Agency "initial" reviews of their records for Automatic Declassification under EO 13526 (Section 3.3), and interagency reviews of declassified records at the National Archives and Records Administration's National Declassification Center, and thereby potentially attain lifecycle cost avoidance by negating the need for re-reviews of those records containing FRD.

It is important to note that this initiative does not include the declassification of any information relating to the design, manufacture, or utilization of nuclear weapons.

Defense Advanced Research Projects Agency (DARPA) Open Catalog

For the latest information, click on
http://open.defense.gov/Transparency/DARPAOpenCatalog.aspx

The DARPA Open Catalog contains a curated list of DARPA-sponsored software and peer-reviewed publications. DARPA funds fundamental and applied research in a variety of areas including data science, cyber, anomaly detection, etc., which may result in reusable technology that can benefit multiple government domains. The goal of the Open Catalog is to make these reusable technologies available to other branches of government and the general public, when possible, to promote efficiency and effectiveness in developing national capabilities. The DARPA Open Catalog organizes publically releasable material from DARPA programs. DARPA has an open strategy to help increase the impact of government investments.

DARPA is also interested in building communities around government-funded software and research. The creation of the Open Catalog will help enable the development of these communities by directing interested web traffic to the code repositories for this software. This will enhance the ability of nontraditional partners to leverage these software tools, by increasing the exposure to the software and thereby increasing the potential for a community to develop around any particular piece of code. DARPA and the larger government will benefit from the development of these communities, who will hopefully test and evaluate elements of the software and afterward adopt them as either standalone offerings or as components of their products.

More broadly, a goal is to establish a modern technology base-- including better starting positions for new/small labs/companies, collaborative projects, cross-community applications, transparent performance evaluation, and interoperability.

The Open Catalog initially went live in early February 2014 with software and publications that were developed under the XDATA program. Since then, the Catalog has expanded to contain all of the programs with releasable content under the Information Innovations Office (I2O), which in addition to open source software included software for government purposes only, complied software (binaries), experimental results, data, and various kinds of publications. If the Research and Development community shows sufficient interest, DARPA will continue to make available information generated by DARPA programs, including software, publications, data, and experimental results.

Section V – Conclusion

Public and Agency Ideas

As stated previously, this document is a work in progress with additional information constantly updated on our Open Government website located at *http://www.defense.gov/open*. We welcome and encourage feedback from DoD employees, other Federal agencies and especially from the public and Civil Society. You will find a feedback form at: *http://open.defense.gov/ContactUs.aspx*.