DoD Open Government Plan Version 4.0

September 15, 2016

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 [https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment]. This memorandum announced the Administration's commitment to creating openness in the government by operating under the principles of transparency, participation, and collaboration. As part of its commitment to an open government, the Administration issued the first U.S. Open Government National Action Plan (NAP) in 2011, and followed up with its second NAP in 2013. On October 27, 2015, the White House released its third NAP (NAP 3.0) building upon initiatives published in the first and second NAPs, and included additional requirements, such as implementing the Controlled Unclassified Information Program and providing for increased public access to federally funded research information.

The Office of the Management and Budget (OMB) also issued an Open Government Directive (M-10-06) in December 2009, requiring agencies to issue their own Open Government Plans, and followed up with subsequent memoranda for agencies to provide updates to such Plans. The Department of Defense (DoD) utilizes the Department's Open Government website [http://www.defense.gov/open to provide information on an on-going basis about its open government initiatives. With this Open Government Plan, DoD provides information on its ongoing and anticipated efforts to increase openness and transparency in furtherance of the principles outlined by the President's Memorandum.

Department of Defense Involvement in Open Government Activities

DoD has, in many ways, led in transparency efforts for decades and has been committed to promoting openness to the American public as it carries out its missions. For example, DoD's broadcasting studios include major news organizations within its headquarters. The American public would likely have seen the Secretary of Defense and the Chairman of the Joint Chiefs of Staff sharing a briefing podium in the Pentagon Briefing Room on the nightly news, as well as seen news correspondents embedded with combat units reporting from "somewhere in" the war zone during combat operations.

The DoD Open Government plan, outlined below, is an extension of this long-standing commitment. The Plan provides updates to certain initiatives, such as in the areas of Freedom of Information Act and Privacy, and provides new information on initiatives, such as in the areas of Open Innovation Methods, Access to Scientific Data and Publications, and Open Source Software. The DoD plan is, by its nature, evolving and is intended to be viewed in conjunction with the Department's Open Government website [http://www.defense.gov/open]. This webpage, as discussed above, has been used to carry out the Department's open government efforts, and as such is updated to provide the latest information on these initiatives.

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 prohibitive 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, which is managed by the DoD Office of the Chief Information Officer (OCIO).

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 U.S. Army Signal Corps. In modern times, DoD developed and launched the first weather satellite, Vanguard 2, on February 17, 1959 as part of the U.S. 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 forecasting through the U.S. 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

Participation in Proactive Disclosure Release to All Pilot

As part of its 2016 Open Government Initiative, the White House launched the Release to All pilot program. The U.S. Department of Justice (DOJ) was the lead agency and the DoD was one of seven participating federal agencies.

The pilot program was conducted to test the feasibility of "automatically" publishing online the records released to individual requesters under the Freedom of Information Act (FOIA). The pilot agencies explored ways to increase government transparency and give citizens more information about government decisions and policies.

Eight FOIA components within the DoD were selected based on their differing workloads, types of requests, resources available, and agency mission in order to present a comprehensive result of the impact of additional duties on the DoD components. The DoD component participants were: the U.S. Air Force (Air Force), Defense Commissary Agency (DeCA), Defense Finance and Accounting Service (DFAS), Defense Intelligence Agency (DIA), National Guard Bureau (NGB), U.S. Northern Command (NORTHCOM), U.S. Southern Command (SOUTHCOM), and the Office of the Secretary of Defense / Joint Staff Requester Service Center (OSD/JS).

The pilot program was conducted over the course of seven months from August 1, 2015 to January 31, 2016, including one preparation month and six evaluation months. The participating components were provided with several metrics for monthly collection and evaluation. The Department is now working with the DOJ through the Chief FOIA Officers Council as the Administration looks to implement a new policy based on this concept across the federal government by January 2017.

Other Examples of Proactive Disclosure

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 DoD 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

DoD Privacy and Civil Liberties Programs

The DoD is committed to protecting and promoting privacy and civil liberties in its operations and programs consistent with the Department's national defense mission. To ensure compliance with the applicable federal statutes and OMB guidelines for privacy and civil liberties, the Department established the DoD Privacy Program and the DoD Civil Liberties Program. Together, these programs safeguard the privacy and civil liberties of individuals and the personal data entrusted to the Department.

Structure of DoD's Privacy and Civil Liberties Programs

The Deputy Chief Management Officer (DCMO) is the DoD Privacy and Civil Liberties Officer (PCLO) and ensures the Department continues its long-standing tradition of providing leadership dedication and attention to privacy and civil liberties matters. The Directorate for Oversight and Compliance (DO&C) oversees the DoD privacy and civil liberties programs and reports directly to the DCMO about privacy and civil liberties issues that may require action by the DCMO and/or senior Department leaders. The Director of Oversight and Compliance was also designated by the DCMO as the DoD Senior Agency Official for Privacy (SAOP). The Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD), located within the DO&C, performs many privacy and civil liberties functions on behalf of the DCMO and DO&C in their respective roles as PCLO and SAOP. Due to its vast size, the DoD has a decentralized privacy and civil liberties program with each of its components implementing its own programs, under the policy direction of DO&C. This decentralized approach enables DoD-wide compliance with laws, policies, and guidance and helps ensure that privacy and civil liberties are adequately considered in all Department activities.

Examples of DoD Privacy and Civil Liberties Oversight and Compliance Activities:

System of Records Notices (SORNs)

SORNs provide public notice and transparency about personal information collected, used, disseminated, and maintained in a system of records. 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 SORN for all DoD systems of records. The public can view DoD SORNs on the DPCLTD web page at http://dpcld.defense.gov/Privacy/SORNs.aspx.

The Senior Agency Official for Privacy (SAOP) portion of DoD's annual Federal Information Security Modernization Act (FISMA) of 2014 Report

DoD's annual FISMA report includes input from the SAOP, the Office of the Chief Information Officer (CIO), and the DoD Inspector General (IG). The CIO compiles the report and submits it to 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 and related FISMA documents are available on the OMB Office of E-Government and Information Technology web page at http://www.whitehouse.gov/omb/e-gov/docs.

DoD Privacy and Civil Liberties Officer Report

Section 803 of Public Law 110-53, "Implementing Recommendations of the 9/11 Commission Act of 2007 (42 U.S.C. 2000ee-1)," requires DoD to submit periodically, but not less than semi-annually, a Privacy and Civil Liberties Report to Congress and the Privacy and Civil Liberties Oversight Board (PCLOB). The public can access these reports on the DPCLTD web page at http://dpcld.defense.gov/Reports/.

Annual 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 Annual Computer Matching Activity Report is submitted to OMB and to Congress. The public can access these reports on the DPCLTD web page at http://dpcld.defense.gov/Reports/.

Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" Report

Executive Order 13636 requires each federal department and agency to develop and implement privacy and civil liberties safeguards in concert with their cybersecurity activities. Each agency's senior official for privacy and civil liberties is required to conduct annual assessments of those safeguards. DoD submitted its privacy and civil liberties assessment of the Defense Industrial Base Cybersecurity/Information Assurance Program to the Department of Homeland Security for inclusion in the 2016 public report. The 2016 public report can be found at https://www.dhs.gov/publication/executive-order-13636-privacy-civil-liberties-assessment-report-2016.

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 DoD was certified by the U.S. Office of Special Counsel as having completed the 2302(c) Whistleblower Act Certification Program [https://osc.gov/pages/2302cregistered.aspx] 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 IG can investigate alleged reprisal against those whistleblowers.

Employees must take "Notification of Anti-discrimination and Retaliation (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 http://www.defense.gov provides visitors with a knowledge base to address a variety of subjects related to the Department of Defense and the Military services, as well as 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.

Participation in Analytics.USA.gov

Guidance for incorporating the Digital Analytic Program into DoD websites will be addressed in a forthcoming update to DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities" available at http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf. As of the date of this document, there are already 13 public DoD websites on the .GOV domain that participate in the Digital Analytics Program.

Open Innovation Methods

The DoD has long been a leader in open innovation methods. Two new initiatives deserve special consideration:

- The Defense Innovation Unit Experimental (DIUx) is a United States Department of Defense (DOD) innovation aimed at developing a working relationship with technology companies. The initiative started in August 2015 with an office opening at Moffett Federal Airfield, California. In May 2016, Secretary Carter announced he would be opening another Innovation Hub in the Boston Area. The DIUx mission is to serve as a local point-of-presence, perform technology scouting, and build relationships. Further information is available at: https://www.diux.mil/.

- The Defense Digital Service (DDS) was established to drive game-changing evolution in the way DoD builds and deploys technology and digital services. The DDS exists to apply best-in-class private sector practices, talent, and technology to transform the way software products are built and delivered within DoD. The DDS works closely with stakeholders in

the DoD and other government entities and has a close relationship with the United States Digital Service in the Executive Office of the President.

Access to Scientific Data and Publications

In February 2013, the 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 support increased access to the results of research funded by the federal government. As DoD's central resource for the collection, preservation, protection, analysis, and broad dissemination of DoD-funded technical information the Defense Technical Information Center (DTIC) was tasked with implementing the infrastructure to collect and disseminate the journal articles and manuscripts that are the result of DoD-funded research. In July 2014, the Undersecretary of Defense for Acquisition, Technology and Logistics released a Memorandum on Public Access that directed all DoD components to comply with the OSTP memorandum. In March 2015, DoD released the DoD Plan to Establish Public Access to the Results of Federally Funded Research (http://www.dtic.mil/dtic/pdf/dod_public_access_plan_feb2015.pdf). DTIC introduced an initial collection of journal articles and manuscripts for the public in September 2015 through a public access informational page and search that leverages the CrossRef/CHORUS feed. A new web-based submission form [http://www.dtic.mil/dtic/submit/submit.html] was introduced in April 2016 to begin accepting voluntary submissions of journal articles and citations. The current collection includes: 2,076 full text journal articles, 3,307 citations (https://publicaccess.dtic.mil), 33,465 full text journal articles in DTIC legacy collection [http://www.dtic.mil/dtic/search/tr/journal.html] and 479,100 publicly available items in the DoD Technical Reports collection [http://www.dtic.mil/dtic/search/advanced_search.html].

Other DTIC resources available to the public

DTIC Search [http://www.dtic.mil] provides access to more than 1 million reports on Defense-funded research, development, and test and evaluation activities.

DoD Investment Budget Search [http://www.dtic.mil/dodinvestment] provides the budgetary and narrative information included in the President's Budget Submissions and Justification Books for DoD research, development, test and evaluation, and procurement investments.

Defense Innovation Marketplace [http://www.defenseinnovationmarketplace.mil] is an industry resource for DoD research and engineering investment priorities. The Marketplace contains DoD R&E strategic documents, solicitations, business opportunities, technology interchange meetings, small business resources, news, and events.

Open Source Software

The DoD issued guidance for using Open Source Software internally in 2009. The guidance is available at: http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf. It is supplemented by a large collection of Frequently Asked Questions available at http://dodcio.defense.gov/Open-Source-Software-FAQ/.

One of DoD's Flagship Initiatives from the last version of its Open Government Plan was the Defense Advanced Projects Research Agency (DARPA) Open Catalog. This is a list of DARPA-sponsored software and peer-reviewed publications. Many of the programs include

source code listings for download and use by the public. More information and a list of the programs and source code is available at: http://opencatalog.darpa.mil/.

Additionally, many DoD projects have contributed their code to GITHUB and other not-for-profit organizations. Examples include:

- https://github.com/ozoneplatform
- https://github.com/redhawksdr
- https://github.com/missioncommand
- https://accumulo.apache.org/
- http://codice.org/ddf/

Spending Information

The Digital Accountability and Transparency Act of 2014 (DATA Act) goal is to increase government spending transparency. It expands the Federal Funding Accountability and Transparency Act of 2006, vastly increasing the level of searchable, detailed information on contract and grants. Effective May 2017, the DATA Act reflects heightened congressional interest in reporting, begun with the American Recovery and Reinvestment Act of 2009. The Department has been working for the past two years to prepare its financial information to be available to the public by the effective date in May 2017.

DATA Act implementation is complementary to our audit readiness effort, providing spending transparency on top of validated financial management stewardship. DATA Act reporting is not a separate requirement for the DoD, but a facet of the overall effort to standardize and improve the financial information being made available to decision makers in the Department and which will now be available to the public in an easy and accessible format on a web-site to be maintained by the U.S. Department of the Treasury.

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 - https://www.navy.com/social-media.html
- 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.defense.gov/Video

Public Notice

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

There are many existing programs and Internet presences that the public 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 the Secretary of Defense and other senior leaders is regularly highlighted at http://www.defense.gov/News/Special-Reports/Travels-with-the-Secretary.

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.osd.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.

Family and Employer Programs and Policy

Family and Employer Programs and Policy (FEPP) is a staff group within the Office of the Assistant Secretary of Defense for Manpower and Reserve Affairs, comprised of Employer Support of the Guard and Reserve (ESGR), the Yellow Ribbon Reintegration Program (YRRP), and Service Member and Family Readiness (SMFR.) Together, this partnership of programs serves as a readiness enabler for National Guard and Reserve Service members, their families, and employers. Moreover, these programs provide a voice for the Reserve Components (RC) within the Office of the Secretary of Defense for the development of programs, policies, and laws that impact quality-of-life issues.

FEPP is the go-to resource for the latest information regarding the catalog of programs, benefits, and entitlements that impact the Reserve community. Each program in the Department of Defense portfolio is relied upon by RC leaders to address family and employment concerns:

- ESGR seeks to promote a culture in which all American employers support and value the employment and military service of RC members. ESGR, with committees in all 54 states and territories staffed by more than 4,500 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. For more information visit www.ESGR.mil and www.FreedomAward.mil.

- YRRP promotes the well-being of National Guard and Reserve members, their families, and communities by connecting them with resources throughout and beyond the deployment

cycle. YRRP provides flexible tools for RC leaders to address the deployment and reintegration concerns of Service members and their families. Each RC executes YRRP events around the globe based on their needs supported by curriculum, tools, and best practices developed and maintained by the YRRP Center for Excellence at www.YellowRibbon.mil. RC members and their families can find and register for YRRP events by visiting www.YellowRibbonEvents.org.

- SMFR helps maintain a ready and resilient force that successfully navigates the challenges of RC service. It does this by empowering families through local service providers, connecting them to resources, and ensuring high quality services and resources are easily accessible. SMFR is also focused on policy oversight, which includes ensuring that, as policy is implemented, it applies to the RC. The use of joint program standards, standardized assessment tools, and quality family readiness service provider training for the RC is a priority for SMFR.

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://pentagontours.osd.mil/tours] 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 at least 14 days in advance through the website above.

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

The DoD Chief Information Officer develops and establishes DoD policy and standards to implement a DoD Records Management Program 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 Instruction 5015.02, "DoD Records Management Program" (http://www.dtic.mil/whs/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/tagResults.aspx?ID=37.

- The Department of the Air Force's key documents for records management include Air Force Instruction (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, "Records Management Policy for the Joint Staff and Combatant Commands," 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, "OSD Records and Information Management Program," available at http://www.dtic.mil/whs/directives/corres/pdf/a015p.pdf.

Freedom of Information Act (FOIA) Requests

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

DoD's Support of FOIA

DoD continues to maintain a high level of support for FOIA. At this year's Sunshine Week recognition ceremony hosted by the DOJ, DoD personnel took home both a team FOIA Exceptional Service Award and an individual FOIA Lifetime Service Award. DoD was also one of the seven agencies that volunteered to participate in the "Release to One is a Release to All" pilot program with eight of DoD's Component FOIA Requestor Service Centers testing the concept and providing feedback to DOJ.

Overall Structure

The DoD Chief FOIA Officer is the DCMO. On behalf of this senior official, the DO&C 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, DO&C is responsible for the formulation and implementation of FOIA Policy for the Department on behalf of the DoD Chief FOIA Officer. Due to its size and complexity, the DoD FOIA Program is decentralized, with operations at numerous FOIA Requester Service Centers worldwide. Each DoD Component operates at least one FOIA Requester Service Center 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 DoD FOIA Policy website, available at *http://open.defense.gov/Transparency/FOIA/,* as well as https://www.foia.gov/, provide links to the DoD FOIA Requester Service Centers and a listing of FOIA Public Liaisons 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 at http://open.defense.gov/Transparency/FOIA/FOIA-Handbook/.

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 Libraries

DoD Components maintain electronic FOIA Libraries in accordance with 5 U.S.C. §(a)(2)(D), where agencies are required to post documents that have been requested three or more times. On our Open Government website, DoD also added links to the major FOIA Reading Rooms maintained across the Department, which contain frequently requested material and are regularly updated. They can be found at http://open.defense.gov/Transparency/FOIA/Find-An-Office/.

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 6,593 requests, exceeding the 10% per year goal by 239 requests.

At the end of FY 2014, the DoD FOIA backlog increased to 9,493 requests, which was an increase of 44% in two years. Some of the reasons for this increase include reduction in personnel and resources due to sequestration and a 20% reduction of DoD headquarters' operation budgets, allocation of resources from FOIA processing to FOIA litigation, increasing complexity of FOIA requests and documents, and increases in FOIA requests with DoD Components of the Intelligence Community due to disclosures in recent years.

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 DoD 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. DPCLTD is responsible for operating the DoD FOIA Program, and has implemented a three-pronged approach to training. DPCLTD holds FOIA/Privacy Act Training Workshops at different geographical locations that have a concentration of DoD personnel. These three-day workshops are held at military installations or other locations that do not have additional conference fees. In the past few years, DPCLTD has hosted workshops in Alexandria, VA; Ft. Sam Houston, San Antonio, TX; MacDill AFB, Tampa, FL; and Germany. Planned workshops for the next year include Travis AFB in northern California, Italy, Hawaii, and Knoxville, TN.

DPCLTD also holds several training sessions through the Defense Collaborative Services (DCS) medium, which is described below. DCS is utilized 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. These training sessions are recorded for future use. Second, DPCLTD holds "FOIA Chat" sessions where, in a real time format, participants from around the world can ask questions of the presenter. In addition, participants can engage in informative discussions with other participants while one or more experienced FOIA experts are available for questions, 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 attorneys 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 DOJ online FOIA training modules became available, the DoD immediately made them available to all DoD personnel online via Joint Knowledge Online (JKO), which is the DoD unique and authoritative source for online joint training. Additionally, many DoD Components made the videos available on their individual e-learning platforms.

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. 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

DoD 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.

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: https://www.archives.gov/declassification/ndc/final-prioritization-plan.pdf.

- Biannual Report on Operations of the National Declassification Center, available at: https://www.archives.gov/declassification/ndc/reports/ (includes current and previous reports).

Public Participation

For the latest information, click on
http://open.defense.gov/Transparency/Electronic-Rulemaking/

Rulemaking

The DoD Directive-type Memorandum DTM-06-008, April 30, 2006, Federal Docket Management System, directed all of the Department's entities to use the online Federal Docket Management System (FDMS), a component of the federal e-Rulemaking Initiative, for their public regulatory proceedings. By implementing FDMS, DoD's internal rulemaking business processes are more transparent and open for public participation. The DoD online regulatory program includes several federal websites that contain important and diverse elements of the regulatory docket.

Regulations.gov is e-Rulemaking's public-interfacing website providing citizens, small businesses, corporations, civic organizations, and all levels of government with one-stop access to review and comment electronically on DoD proposed rulemaking actions that are currently open for comment. Interested parties can access the daily Federal Register [FederalRegister.gov] to view publication of DoD regulatory documents in the following categories: "Pending Publication", "Significant Regulations", "Recent Articles", "Closing Soon", and "Documents Opening".

- Interested Parties can access RegInfo.gov to learn about current and past DoD rules that went to the Office of Management and Budget/Office of Information & Regulatory Affairs (OMB/OIRA) for review and analysis. Interested parties can also use this website to review the Fall 2011 Regulatory Plan and Unified Agenda of Federal Regulatory and Deregulatory Actions and the Spring 2011 Unified Agenda of Federal Regulatory and Deregulatory Actions

- The DoD Issuances Website, [http://www.dtic.mil/whs/directives/] is the official DoD source for electronic publication of DoD issuances; however, interested parties can also access applicable DoD forms, directives, and instructions from this website.

Challenges and Competitions

DoD regularly sponsors challenges and competitions, especially through the Defense Advanced Research Projects Agency (DARPA). For information on current opportunities to participate, click on http://www.challenge.gov or visit the DARPA website at http://www.darpa.mil.

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).

Defense Collaboration Services (DCS)
DCS is the DoD's designated enterprise tool for worldwide synchronous and asynchronous enterprise collaboration. The DCS tool provides web conferencing (session management, text messaging, application sharing/broadcasting, audio, presence and awareness, voting/polling, video, multiple sessions, and recording), and Instant Messaging (IM) for users across the Department enterprise. DCS can scale to handle 10,000 concurrent users with a maximum of 250 participants per web conference.

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 Portal.

Other Collaboration Platforms
DoDTechSpace [https://www.dtic.mil/dodtechspace] is a virtual workspace for the DoD science and technology enterprise. Available to authorized DoD and Federal Government employees and contractors this tool provides a platform to share information, collaborate on projects and discuss innovative solutions.

DoDTechipedia [https://www.dodtechipedia.mil] is a science and technology wiki for authorized DoD and federal government employees and contractors to share and store research information, updates or trends.

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 NAP (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 jointly developed a process and has begun 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 also 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 discussed above, the DoD Open Government plan is an evolving document with additional information updated on the DoD 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.

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