

# Department of Defense

## Section 1: Highlights of Agency E-Government Activities

### A. Enhanced Delivery of Information and Services to the Public - Sec. 202(g)

*Section 202(g) of the E-Gov Act requires agencies to provide information on how electronic Government is used to improve performance in delivering programs to constituencies. In no more than 250 words, describe one IT agency activity or initiative that enhances the delivery of information and services to the public and others, or makes improvements in government operations. This example should highlight how electronic government improved the effectiveness, efficiency, and quality of services provided by your agency.*

In 2015, the Defense Information Systems Agency (DISA) leveraged the assorted capabilities/ lower costs of the milCloud Infrastructure as a Service solution to roll out a new online collaboration tool called Defense Collaboration Services (DCS). DCS offers DOD employees anywhere in the world (with applicable credentials) secure web conferencing and secure instant messaging, and chat capabilities. milCloud offers value to DOD mission partners by reduced infrastructure costs of operations achieved by the consolidation of virtual environments into DISA's secure Defense Enterprise Computing Centers. Specifically, milCloud is a cloud-services product portfolio, managed by the DISA that features an integrated suite of capabilities designed to drive agility into the development, deployment, and maintenance of secure DOD applications. milCloud leverages a combination of Commercial off-the-shelf and government developed technology to deliver cloud services tailored to DOD requirements. All milCloud products feature the following capabilities: - On-Demand, Self-Service: Consumers can place orders on-demand through web-based self-service tools, configure infrastructure resources where appropriate, and manage their mission application's lifecycle running on those resources without manual intervention from DISA milCloud staff. - Broad Network Access: All products and services have connectivity to the DOD Information Networks, and are configured per relevant DOD security guidelines and approved protocols. - Resource Pooling: Resources are pooled so multiple mission partners consume units from pools provisioned by DISA, enabling efficient use of resources and greater consumption flexibility. - Rapid Elasticity: Portfolio has the ability to expand or contract resource use within virtual resource pools.

### B. Public Access to Electronic Information - Sec. 207(f)(1)(B)

*Section 207(f)(1)(B) of the E-Gov Act requires that agency websites assist public users to navigate agency websites, including the speed of retrieval of search results and the relevance of the results. Provide the updated URL(s) that contains your agency's customer service goals and describes activities that assist public users in providing improved access to agency websites and information, aid in the speed of retrieval and relevance of search results, and uses innovative technologies to improve customer service at lower costs. For example, include the URL to your agency's Customer Service Plan.*

Public Facing Agency URL(s)	Brief Explanation (if necessary)
<a href="http://open.defense.gov/OpenGovernment@DoD/Open">http://open.defense.gov/OpenGovernment@DoD/Open</a>	The goal of customer service in

Public Facing Agency URL(s)	Brief Explanation (if necessary)
<a href="#">GovernmentPlan.aspx</a>	DOD is to ensure customers receive increasingly better service via process improvements and supporting technologies that focus on timeliness, accuracy, and responsiveness. Supporting this goal, the DOD Open Government Plan
<a href="http://www.defense.gov/">http://www.defense.gov/</a>	Defense.gov is the DOD's premier public information site for the dissemination of all current DOD information. Includes URLs to products, directories, inventories, management tools, and other useful information.

## Section 2: Compliance with Goals and Provisions of the E-Gov Act

### A. Performance Integration - Sec. 202(b)

*The E-Gov Act requires agencies to develop performance metrics that demonstrate how electronic government supports agency objectives, strategic goals, and statutory mandates. In no more than 250 words, describe what performance metrics are used and tracked for IT investments and how these metrics support agency strategic goals and statutory mandates. Please discuss performance metrics that focus on customer service, agency productivity, innovative technology adoption and best practices. If applicable, include a description of your agency's evaluation model and how it is used. Provide applicable URL(s) for performance goals related to IT.*

The starting point for performance integration metrics for the DOD is mapping objectives and measures to departmental strategic goals and to the President’s Management Agenda and Federal benchmarking initiatives. The main mechanisms for tracking IT performance and innovation are executed as part of the Department’s Joint Information Environment (JIE) implementation of the Joint Regional Security Stacks, the cybersecurity scorecard process, and in the Defense Business Council’s (DBC) system certification process. JIE metrics focus on implementation of IT infrastructure modernization, improving cybersecurity, and consolidation of data centers. The DBC, co-chaired by the DOD Deputy Chief Management Officer and DOD Chief Information Officer, serves as the principal governance body for defense business operations and as the Department’s Investment Review Board (IRB) for defense business IT systems. This forum oversees application of outcome-oriented performance measures and reviews performance results to track progress against Agency strategic goals and advance efforts to reduce duplication. Various metrics are used in the structured review process of systems by the investment review function of the IRB in support of the review and certification of systems. DOD has implemented a new cybersecurity scorecard process, consistent with the Federal cybersecurity goals, that tracks compliance with cybersecurity standards, configuration, and performance of new security measures to ensure security of the Department’s systems and networks. DOD Instruction 8115.02, “Information Technology Portfolio Management Implementation,” provides the policy and procedural foundation for analysis, selection, control, and evaluation of IT investment portfolios, focusing on improving DOD capabilities and mission outcomes while eliminating duplication.

### B. Accessibility - Sec. 202(c) and (d)

*The E-Gov Act requires agencies to consider the impact of implementing policies on persons without access to the internet, and ensure accessibility to people with disabilities. Provide the URL(s) for your agency's website which describes actions taken by your agency in accordance with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d).*

Public Facing Agency URL(s)	Brief Explanation (if necessary)
<a href="http://dodcio.defense.gov/DoDSection508.aspx">http://dodcio.defense.gov/DoDSection508.aspx</a>	The webpage provides links to DOD Section 508 policy documents, best practices, and points of contact.
<a href="http://dodcio.defense.gov/DoDSection508/Std Stmt.asp">http://dodcio.defense.gov/DoDSection508/Std Stmt.asp</a>	Posting of the DOD accessibility

Public Facing Agency URL(s)	Brief Explanation (if necessary)
<a href="#">X</a>	statement on DOD websites demonstrates the Department's commitment to making electronic and information technologies accessible to individuals with disabilities.

### **C. Government-Public Collaboration - Sec. 202(e)**

*The E-Gov Act requires agencies to sponsor activities that use information technology to engage the public in the development and implementation of policies and programs. In no more than 250 words, describe one example of how your agency utilized technology to initiate government-public collaboration in the development and implementation of policies and programs.*

The DOD continues to use the Federal eRulemaking portal to facilitate public participation in its regulatory process. The Federal eRulemaking portal assists the public with locating, viewing, understanding, and commenting on federal regulatory actions and rulemaking materials. Also, the portal enables the Department's action officers to view and analyze comments received from multiple sources. The DOD processes and tracks approximately 100 rules and 300 to 400 notice documents annually. Additionally, the Department uses the portal to take comment on significant guidance documents, demonstration projects, information collections requiring approval by OMB in accordance with the Paperwork Reduction Act, and Privacy Act System of Records Notices.

### **D. Credentialing - Sec. 203**

*The E-Gov Act seeks to achieve interoperable implementation of electronic signatures for appropriately secure electronic transactions with Government. In no more than 250 words, describe current activities your agency is undertaking to achieve the interoperable implementation of electronic credential authentication for transactions within the Federal Government and/or with the public (e.g. agency implementation of HSPD-12 and/or digital signatures).*

In the past year, DOD has continued its efforts to encourage and enable the use of interoperable Public Key Infrastructure (PKI) credentials. DOD has used PKI for authentication and authorization for a number of years, creating the world's largest implementation of PKI. DOD recognizes the value of PKI for secure identification, digital signing, data encryption, as well as for more efficient and more secure electronic commerce. DOD assists other Federal agencies and its industry and international partners to implement their own PKI systems. Homeland Security Presidential Directive-12 requires most Federal agencies to implement more secure physical and electronic identification systems. Other Federal agencies look to DOD for leadership and guidance in developing their own PKI systems, as well as to benefit from the lessons learned and PKI best practices that DOD has developed. In addition to DOD's efforts to spread the use of PKI in the Federal government, the Department also encourages and promotes the use of PKI by private industry, including its key Defense Industrial Base partners. For several years, DOD has required its key English-speaking allies (Canada, the United

Kingdom, Australia, and New Zealand) to implement their own unclassified and classified PKI systems, so that they can share information securely with DOD. DOD has also developed technologies to use PKI on mobile devices, such as cell phones and tablets. Mobile devices present unique technical and security challenges to incorporating PKI; however, DOD recognizes the benefit of mobile computing and communication, and is adapting PKI to those environments.

**E. USA.gov activities - Sec. 204 and Sec. 207(f)**

*In accordance with Section 204 of the E-Gov Act, www.USA.gov serves as an integrated internet-based system for providing the public with access to government information and services. In accordance with Section 207(f)(3), provide the URL(s) your agency's activities on www.USA.gov.*

Public Facing Agency URL(s)	Brief Explanation (if necessary)
<a href="http://www.usa.gov/Agencies/Federal/Executive/Defense.shtml">http://www.usa.gov/Agencies/Federal/Executive/Defense.shtml</a>	Link to DOD presence on USA.gov.

**F. eRulemaking - Sec. 206**

*The E-Gov Act seeks to assist the public, including the regulated community, in electronically submitting information to agencies under Federal requirements, by reducing the burden of duplicate collection and ensuring the accuracy of submitted information. In no more than 250 words, provide a description of your agency's use of online electronic regulatory submission capabilities, specifically the usage of www.Regulations.gov and the Federal Docket Management System (FDMS).*

DOD continues to use the eRulemaking Federal Docket Management System (FDMS) and Regulations.gov to increase citizen access and participation in its regulatory process. FDMS provides for document management and analysis with an electronic record-keeping capability. Regulations.gov provides citizens a user-friendly web form to submit comments and supporting documents, offers simple and sophisticated searches, bookmarking, email notifications, and other social media tools. These online capabilities enhance the public's knowledge of what rules and notices are open for comment and provide for the electronic submission of comments to relevant decision-makers. Additionally, these online capabilities allow the public to access regulatory supporting materials that facilitate the preparation of more informed public comments, which are clearer and increasingly valuable to decision-makers.

**G. National Archives Records Administration (NARA) Recordkeeping - Sec. 207(d-e)**

*The E-Gov Act requires agencies to adopt policies and procedures to ensure that chapters 21, 25, 27, 29, and 31 of title 44, United States Code, are applied effectively and comprehensively to Government information on the Internet and to other electronic records. In no more than 250 words, describe your agency's adherence to NARA recordkeeping policies and procedures for electronic information online and other electronic records. Additionally, please indicate the number of electronic records that have been scheduled with NARA and any pending scheduling for electronic systems at your agency.*

The DOD continues to improve its capabilities for managing electronic records via policy updates and ongoing implementation efforts by DOD Components. - In 2015, the DOD updated DOD Instruction (DODI) 5015.02, "DoD Records Management Program" to enhance guidance for addressing the challenges of managing the high volume of electronic records within the DOD. This policy requires records management to be incorporated as an integral part of new IT systems development and during significant IT system upgrades; incorporation will be accomplished through a combination of targeted electronic records management solutions and functionality that is designed into electronic systems, such as task management and/or case management systems. DODI 5015.02 also requires annual records management overview training for all DOD employees; this training is consistent with the training goals set forth in OMB Memorandum M-12-18, "Managing Government Records Directive." - DOD Components continue efforts to improve their electronic (email and permanent) records management capabilities in alignment with the goals set forth in OMB Memorandum M-12-18; progress toward meeting these goals is reported through the annual DOD Senior Agency Official Report to NARA. Reporting on the scheduling of DOD electronic records is included in the annual Records Management Self-Assessment that is submitted to NARA.

**H. Freedom of Information Act (FOIA) - Sec. 207(f)(A)(ii)**

*The E-Gov Act requires agency websites to include direct links to information made available to the public under the Freedom of Information Act. Provide the updated URL for your agency's primary FOIA website.*

Public Facing Agency URL(s)	Brief Explanation (if necessary)
<a href="http://open.defense.gov/Transparency/FOIA.aspx">http://open.defense.gov/Transparency/FOIA.aspx</a>	Link to DOD Open Government/Freedom of Information Act webpage

**I. Information Resources Management (IRM) Strategic Plan - Sec. 207(f)(A)(iv)**

*The E-Gov Act requires agency websites to include the strategic plan of the agency developed under section 306 of title 5, US Code. Provide the updated URL to your agency's IRM Strategic Plan. This plan should encompass activities in FY14. If your agency does not have an updated plan, please provide the URL to the most recent plan and indicate when an updated plan will be available.*

Public Facing Agency URL(s)	Brief Explanation (if necessary)
<a href="http://dodcio.defense.gov/Library.aspx">http://dodcio.defense.gov/Library.aspx</a>	Link to DOD IRM Strategic Plan

**J. Research and Development (R&D) - Sec. 207(g)**

*If your agency funds R&D activities, provide the updated URL(s) for publicly accessible information related to those activities, and specify whether or not each website provides the public information about Federally funded R&D activities and/or the results of the Federal research.*

Public Facing Agency URL(s)	Brief Explanation (if necessary)
<a href="http://www.dtic.mil/dtic/">http://www.dtic.mil/dtic/</a>	Defense Technical Information Center.s (DTIC) Research & Engineering (R&E) Gateway offers a collaborative environment, where DOD and industry partners, separated by geography, time and organization, can access and contribute information and data. The sit
<a href="http://www.dtic.mil/dodinvestment">http://www.dtic.mil/dodinvestment</a>	This database furnishes the DOD investment budgetary/narrative information from the President's Budget Submissions or Justification Books. Investment budgets include both Research, Development, Test and Evaluation (RDT&E) and Procurement. RDT&E programs
<a href="http://comptroller.defense.gov">http://comptroller.defense.gov</a>	The R&D funding information can be accessed via .Budget Materials. module and is derived from and consistent with the Comptroller Information System database. It provides Department of Defense.s R&D budget information and does NOT provide the public info

### **K. Privacy Policy and Privacy Impact Assessments - Sec. 208(b)**

*The E-Gov Act requires agencies to conduct a privacy impact assessment; ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and if practicable, after completion of the review under clause, make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means. In no more than 250 words, describe your agency's adherence to this provision, including adherence to OMB's guidance pertaining to the use of IT to collect, maintain, or disseminate identifiable information, or when new systems are procured for this purpose. In addition, describe your agency's process for performing and updating privacy impact assessments for IT.*

The Defense Privacy and Civil Liberties Division (DPCLD) works with DOD CIO to ensure that DOD meets OMB privacy compliance requirements for completion of, and updates to, System of Records Notices (SORNS) and Privacy Impact Assessments (PIAs). DPCLD and DOD CIO collaborate on Federal Information Security Management Act quarterly and annual reporting, which includes reviews of SORNS and PIA compliance across DOD. The DOD PIA program protects the privacy of individuals by systematically ensuring that controls are in place to protect data. The Department's assessments help ensure that vulnerabilities of DOD information

systems containing Personally Identifiable Information (PII) are minimized. DOD PIA Program: DOD Instruction 5400.16 “DOD Privacy Impact Assessment (PIA) Guidance,” establishes PIA policy and procedures to reflect current and emerging requirements. - Ensures PIAs are conducted on all electronic collections of PII and adequate controls are in place to protect public and Federal employees’ PII. - Provides continuous outreach, training, and education to DOD Components to assist with establishing and maintaining PIA programs that increase the completion rate of PIAs in compliance with the law. - Requires PIAs to be performed and updated as necessary when a system change creates new privacy risks including, but not limited to, significant system management changes, new public access, conversion from paper-based records to electronic systems, and significant merging of data sources. Every three years, a PIA must be reevaluated to ensure any changes to the system that could impact privacy are reviewed and updated as part of the certification and accreditation process.

**K2. Privacy Policy and Privacy Impact Assessment Links - Sec. 208(b)**

*In addition to the narrative provided above in section K., provide the updated URL(s) for your agency's privacy policy and the website where your agency's privacy impact assessments are available.*

Public Facing Agency URL(s)	Brief Explanation (if necessary)
<a href="http://dpcl.d.defense.gov/Privacy/Resources.aspx">http://dpcl.d.defense.gov/Privacy/Resources.aspx</a>	Link to DOD Privacy Policy and guidance.
<a href="http://dodcio.defense.gov/InTheNews/PrivacyImpactAssessments.aspx">http://dodcio.defense.gov/InTheNews/PrivacyImpactAssessments.aspx</a>	Link to DOD Component Privacy Impact Assessments (PIAs).

**M. Agency IT Training Programs - Sec. 209(b)(2)**

*The E-Gov Act calls for agencies to establish and operate information technology training programs. The act states that such programs shall have curricula covering a broad range of information technology disciplines corresponding to the specific information technology and information resource management needs of the agency involved; be developed and applied according to rigorous standards; and be designed to maximize efficiency, through the use of self-paced courses, online courses, on-the-job training, and the use of remote instructors, wherever such features can be applied without reducing the effectiveness of the training or negatively impacting academic standards. In no more than 250 words, describe your agency's IT training program, privacy training program, cross-agency development programs, and competencies reviews for IT workforce.*

In April 2015, the Department issued the DOD Cyber Strategy with focused initiatives to maintain a strong, well-trained military and civilian cyber workforce. In addition, a new policy directive, DODD 8140.01, “Cyberspace Workforce Management,” was published in August 2015. This governance document supports the longer-term development of cyber workforce qualification requirements. In the interim, DOD continues to maintain its Information Assurance (IA) Workforce Improvement Program, which guides the training and qualifications requirements for over 22,000 DOD civilians. The Department has technical schoolhouses run by the Military Services and Combat Support Agencies, and six academic institutions, which provide graduate-level IT/cyber education programs. Commercial training and certification programs provide



baseline IA/cybersecurity knowledge for designated jobs. Further, DOD participates with DHS to provide online, on-demand training through the Federal Virtual Training Environment (FedVTE). DOD meets Privacy Act (PA) training requirements of OMB Circular A-130, "Management of Federal Information Resources," and DOD 5400-11R, "Department of Defense Privacy Program" through an online privacy general awareness course, a 3-day PA Compliance & Management course; System of Records Notice and Breach Management training workshops; and a PA Essentials course. DOD Components also provide annual and refresher PA training. In FY 2015, DOD finalized baseline competencies for the 1550 Computer Science series and initiated work on competencies for the 0335 Computer Clerk and Assistant series, which upon completion, will be loaded into the Defense Competency Assessment Tool for use by individuals and their supervisors. The 0391 Telecommunications series' competencies are scheduled for review in FY 2016.