DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

APR 0 1 2015

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Department of Defense Information Resources Management Strategic Plan

This DoD Information Resources Management (IRM) Strategic Plan Version 1.0 presents the Department's IRM strategic goals and objectives. The IRM Strategic Plan is aligned to the National Defense Strategy and the DoD Strategic Plan contained in the DoD's FY 2015 Budget Request Overview, dated March 2014. The plan meets the Federal requirement for all agencies to establish an IRM Strategic Plan, as specified by Law and various Office of Management and Budget (OMB) Circulars and guidance memoranda. It also addresses additional OMB requirements for agency IRM strategic plans, as specified in OMB's Digital Government Strategy, which lays out actions in a 12-month roadmap to achieve three main objectives:

- Enable the American people and an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, on any device.

- Ensure that as the government adjusts to this new digital world, we seize the opportunity to procure and manage devices, applications, and data in smart, secure and affordable ways.

- Unlock the power of government data to spur innovation across our Nation and improve the quality of services for the American people.

More specifically, this DoD IRM Strategic Plan depicts how DoD's IRM activities support the missions of the Department and ensure that information resource matters are integrated with Departmental organizational planning, budget, procurement, financial management, human resources management, and program decisions. The plan highlights DoD CIO-led efforts that are key enablers for accomplishing the missions of the Department more effectively and efficiently. Foremost among those efforts is implementing the Joint Information Environment, which is designed to re-align and restructure DoD's ability to provide better access to information to the user, improve the Department's ability to defend the networks and the data, and keep pace with constantly changing technological and operational factors.

Attachment:
As stated

DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES
ASSISTANT DIRECTOR OF NATIONAL INTELLIGENCE AND CHIEF INFORMATION OFFICER
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS

Department of Defense Information Resources Management Strategic Plan

Version 1.0

Contents

Executive Summary

PortfolioStat is a tool that Office of Management and Budget (OMB) designed for agencies to use to assess the current maturity of their Information Technology (IT) portfolio management process, make decisions on eliminating duplication, augment current Chief Information Officer (CIO) led capital planning and investment control processes, and move to shared solutions in order to maximize the return on IT investments across the portfolio. To improve the outcomes of PortfolioStat and to mature agency IT portfolio management, OMB is consolidating previously collected IT plans, reports and data calls into three primary collection channels:[1]

- **Information Resources Management (IRM) Strategic Plans** support the Department of Defense (DoD) Strategic Plan, and "provide a description of how information resources management activities help accomplish agency missions, and ensure that information resource management decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions."

- **The Enterprise Roadmap** "documents an agency's [DoD's] current and future views of its business and technology environment from an architecture perspective," by "reflecting the implementation of new or updated business capabilities and enabling technologies that support the agency's strategic goals and initiatives. It also contains a transition plan to show the sequence of actions needed to implement the IRM Strategic Plan. Moreover, it focuses on increasing shared approaches to IT service delivery across mission, support, and commodity areas."

- **An "integrated data collection" channel** for agencies to report structured and quantitative information, "to report agency progress in meeting IT strategic goals, objectives and metrics as well as actual and planned cost savings and avoidances resulting from IT management actions." This channel will aggregate data reported previously under "PortfolioStat, the Federal Data Center Consolidation Initiative (FDCCI), quarterly Federal Information Security Management Act (FISMA) metrics, and the Federal IT Dashboard."

One purpose of IRM strategic planning is to focus DoD (like all Federal agencies) on those goals and related activities that contribute to actual and planned cost savings (or cost avoidance) through the implementation of IT investments guided by the IRM Strategic Plan and Enterprise Roadmap. In particular, the Federal CIO seeks efficiencies, savings, and greater security through agency migration to shared services and cloud solutions, the consolidation of commodity IT, and savings achieved through data center consolidation—all of which the Department is working towards under the umbrella of the Joint Information Environment (JIE). This plan identifies IRM

[1] OMB M-13-09, Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management, March 27, 2013

goals, objectives and strategy elements that will move the Department toward the desired JIE end state.[2]

OMB requests that agencies report on the modularity of IT deployments, time to deliver new IT services to users, the extent that "cut and re-invest" approaches are driving new development, and whether agency information resource planning efforts deliver customer functionality required by the agency's strategic priorities and goals.

The DoD IRM Strategic Plan v1.0 is organized in three primary parts:

- Overview: Presents the DoD CIO Vision and Mission and how the DoD IRM Strategic Plan responds to high-level DoD guidance, and then addresses a range of topics including key initiatives and technologies (particularly those efforts encompassed by the JIE), cybersecurity, and digital government.
- Goals: Provides the seven DoD IRM strategic goals, as well as the objectives to accomplish those goals. Each objective contains a set of strategy elements necessary to achieve that objective. A strategy element defines a focused concentration of activities that are near-term and measurable. The DoD IRM strategic goals support DoD's overall (agency) strategic goals and objectives.
- OMB-required Topics: Development of the DoD IRM Strategic Plan responds to and is aligned with the March 27, 2013 memo from OMB Deputy Director for Management, Jeffrey Zients, which dealt with assessing the maturity and effectiveness of IT management practices and provided guidance for agencies' IRM Strategic Plans and for streamlining agency reporting requirements. While the structure of the IRM Strategic Plan is left to the discretion of each agency, OMB requires that, in addition to meeting agency-specific needs, the IRM Strategic Plan addresses nine specific topics. For some of these topics, this plan addresses specific reporting requirements for the agency's IRM Strategic Plan, as called out in the Federal Digital Government Strategy. The nine required topics are[3]:
    - Agency Strategic Goals and Objectives
    - Improving Services to Customers
    - Governance and Management Processes
    - CIO Authorities
    - Cybersecurity Management
    - Workforce
    - Managing Information as an Asset
    - Commodity IT and Shared Services
    - Accessibility

[2] Consistent with guidance in OMB memo M-13-09, this IRM Strategic Plan covers a time horizon of FY 2014-2018. The contents reflect the Department's IRM vision and goals as understood in FY14. However, recognizing the rapid pace of technological change, the Department may revise the plan prior to 2018.

[3] These nine topics are listed exactly as they appear in OMB M-13-09.

Role of the DoD CIO

The DoD CIO is the Principal Staff Assistant (PSA) and advisor to the Secretary of Defense (SecDef) and Deputy Secretary of Defense for information technology, National Security Systems (NSS) and IRM matters. The DoD CIO is responsible for matters relating to the DoD Information Enterprise (IE), including communications, spectrum management, network operations, information systems, cybersecurity, Position, Navigation, and Timing (PNT) policy, and the DoD information enterprise that supports DoD Command and Control (C2).[4] The DoD CIO is tasked with improving the combat power of the Department—as well as its security and efficiency—by ensuring that the Department treats information as a strategic asset and that innovative information capabilities are available throughout all areas of DoD supporting warfighting, business, and intelligence missions. The DoD CIO is a vital member of the Office of the Secretary of Defense (OSD) staff that helps the Warfighter by fulfilling its PSA and Clinger-Cohen Act roles that guide the Department in the incorporation of more agile, efficient and effective technology and practices.

Vision

DoD and partners securely access information and services they need at the time, place and on approved devices of their choosing.

Mission

We lead the DoD Information Enterprise by defining a shared vision, setting overall policy, and driving the standards for the information infrastructure that support warfighting, business, and intelligence missions.

To accomplish the mission, the DoD CIO:

- Works with key stakeholders across the Department to ensure that information is visible, accessible, and understandable to all authorized users in a trusted environment without regard to location or time.
- As PSA, leads specific information resource capabilities including command and control, communications, IT infrastructure, and Information Assurance (IA), ensuring that these capabilities are architected, engineered, and delivered in a manner that optimizes the Department's mission capabilities, increases the Department's security posture, and makes most effective use of the Department's financial resources.
- Leads DoD's network cybersecurity/information assurance efforts and manages DoD enterprise information sharing risks, while at the same time protecting our information assets.
- Provides guidance and oversight with regard to overall operation and defense of the DoD Information Enterprise.

[4] DoD Directive 5144.02, DoD Chief Information Office (DoD CIO), April 22, 2013

DoD IRM Strategic Plan Goals and Objectives

The DoD IRM Strategic Plan v1.0 goals and objectives presented below support the Department's strategic goals as presented in the Department of Defense Strategic Plan as presented in the DoD FY 2015 Budget Request Overview, dated March 2014:

- Prevail in today's wars
- Prevent and deter conflict
- Prepare to defeat adversaries and succeed in a wide range of contingencies
- Preserve and enhance the All-Volunteer Force
- Reform the business and support functions of the Defense enterprise

More specifically, the DoD IRM goals 1, 2, 3, 5, and 6 directly support the first three of the Department's strategic goals. DoD IRM goal 4 supports the fourth Department strategic goal. DoD IRM goal 5 additionally supports the fifth Department strategic goal.

Goal 1: Exploit the Power of Trusted Information Sharing

Intended Outcome: *Enhanced support to decision making processes—through secure access to DoD information and application of common data standards—improves collaboration both across the DoD enterprise and with external mission partners.*

- **Objective 1: Deploy An Authentication Infrastructure To Dynamically Control Authorized User Access To Information**
  - *Strategy Elements*
    - Oversee and Guide Implementation of Identity and Access Management (IdAM) Infrastructure Capabilities
- **Objective 2: Improve Information Sharing with External Mission Partners**
  - *Strategy Elements*
    - Guide Adoption and Implementation of Secure Information Sharing Technologies, Processes, and Practices
    - Implement An Effective Mission Partner Environment
    - Develop and Publish Interoperability Standards
    - Implement US Government and DoD Safeguarding Initiatives
- **Objective 3: Improve Data Management for Broader Sharing Across the DoD Enterprise**
  - *Strategy Elements*
    - Implement the National Information Exchange Model (NIEM) in DoD
    - Implement Information Exchange Standards
    - Implement Controlled Unclassified Information (CUI)
    - Establish a Data Framework
    - Deploy an effective Records Management System/Program
    - Enable users to leverage Big Data Analytics

- **Objective 4: Improve DoD's Information and Communications Technology (ICT) Support to Contingency Ops**
  - *Strategy Elements*
    - Improve ICT Support to Humanitarian Assistance and Disaster Response, Stability Ops, etc.
    - Provide ICT Support to Asia – Pacific Rebalancing

Goal 2: Improve Operational Effectiveness and Efficiency Through Superior IT Service Delivery

Intended Outcome: *Greater efficiency and broader access to information are achieved through use of a common computing environment, shared services, and mobile applications.*

- **Objective 1: Provide a Common Computing Environment**
  - *Strategy Elements*
    - Define Data Center and IT Infrastructure Architecture
    - Consolidate DoD Data Centers
    - Consolidate IT Infrastructure
    - Establish DoD Enterprise Cloud
- **Objective 2: Deploy Shared and DoD Enterprise IT Services**
  - *Strategy Elements*
    - Improve Accessibility in Accordance with the Rehabilitation Act of 1973, as amended (Section 508), codified at Section 794d of Title 29, United States Code (U.S.C.)
    - Implement Federal Shared Services Strategy
    - Develop and Implement New DoD Enterprise IT Services
    - Implement Unified Capabilities
    - Implement IT Service Management
    - Implement Cross-Domain Services
    - Release and Support an Ozone Widget Framework
- **Objective 3: Enable Agile Decision Making through Mobile Applications**
  - *Strategy Elements*
    - Develop and Implement a Mobile App Store/Mall
    - Develop and Implement Device Native Apps
    - Implement the Requirements of OMB's Digital Government Strategy Milestone 1.2
    - Institutionalize Responsive Design for all DoD Internet Services

Goal 3: Provide a Resilient Communications and Computing Infrastructure

Intended Outcome: *Modernized DoD communications infrastructure provides greater operational and technical resilience, improved interoperability and effectiveness, faster capability delivery, prioritized secure capabilities, and reduced costs.*

- **Objective 1: Improve Communications Networks**
  - *Strategy Elements*
    - Improve Tactical Communications Transport Networking
    - Enable a Joint Aerial Layer Networking Capability
    - Provide Satellite Communications (SATCOM) Diversity and Resiliency
    - Drive Network Standardization/Modernization (including Single Security Architecture (SSA))
    - Optimize Network Operations for Network Situational Awareness
    - Establish and Guide Common Configuration Management
- **Objective 2: Modernize Communications Systems**
  - *Strategy Elements*
    - Modernize Tactical Radios
    - Modernize and Protect PNT
    - Leverage Commercial Technologies and Communications Capabilities
    - Drive Migration to Internet Protocol (IP) version 6
- **Objective 3: Consolidate and Optimize Strategic Gateways**
  - *Strategy Elements*
    - Optimize Strategic Satellite Gateways
    - Establish Beyond Line-of-Sight Capability in Terrestrial Gateways
- **Objective 4: Modernize Defense Information Systems Network (DISN) Transport Infrastructure**
  - *Strategy Elements*
    - Implement Enhanced Voice Over IP (VOIP), Data and Video Services Over Optical Transport Network
    - Optimize the Mix of Military and Commercial SATCOM Capabilities
- **Objective 5: Establish End-to-End SATCOM Capabilities**
  - *Strategy Elements*
    - Deliver Wide-Band SATCOM Capability
    - Deliver Narrow-Band SATCOM Capability
    - Deliver Protected SATCOM Capability
    - Synchronize SATCOM Capability Delivery
- **Objective 6: Integrate Commercial Mobile IT Capabilities**
  - *Strategy Elements*
    - Evolve the DoD Information Enterprise Infrastructure to Support Mobile Devices
    - Enable Communications-On-The-Move and Mobile Networking Capabilities
- **Objective 7: Improve Management of Spectrum**
  - *Strategy Elements*
    - Guide DoD Toward More Efficient Usage and Management of Spectrum
    - Implement a DoD Spectrum Planning and Management System

- **Objective 8: Optimize C2 Systems and Information Sharing Capabilities**
  - *Strategy Elements*
    - Modernize the Family of Joint C2 Capabilities
    - Support Overall Reduction in Joint C2 Costs
    - Synchronize Delivery of Joint C2 Capabilities
- **Objective 9: Ensure National Leadership Command Capabilities (NLCC) Assured Connectivity**
  - *Strategy Elements*
    - Sustain and Modernize Nuclear Command, Control, and Communications
    - Modernize Senior Leader Communications

Goal 4: Evolve the Cyberspace Workforce

Intended Outcome: *A workforce of well-trained, highly qualified professionals supports and defends DoD's Information Enterprise and meets the Department's current, continuously emerging, and expanding mission requirements.*

- **Objective 1: Strengthen the Cyberspace Functional Community Workforce**
  - *Strategy Elements*
    - Improve Cyberspace Workforce Policy and Planning
    - Eliminate Gaps in DoD High-Risk Mission Critical Occupations / Competencies
- **Objective 2: Strengthen the IT Acquisition Workforce**
  - *Strategy Elements*
    - Strengthen IT Acquisition Workforce Competencies
    - Manage, Retool and Implement the IT Program/Project Manager Career Path
- **Objective 3: Enhance Cyberspace Workforce Recruiting, Retention, Education, Training, and Professional Development**
  - *Strategy Elements*
    - Modernize IT Workforce Guidance and Training
    - Refine DoD's Cybersecurity Awareness Program

Goal 5: Improve Oversight and Execution of DoD IT Investments

Intended Outcome: *Increased transparency and accountability for IT investments.*

- **Objective 1: Evolve the DoD Enterprise Architecture and Processes**
  - *Strategy Elements*
    - Develop the DoD Enterprise Architecture and Provide Direction
    - Support Revision of OMB's Federal Enterprise Architecture
- **Objective 2: Manage IT Infrastructure as a Commodity**
  - *Strategy Elements*

- Centralize Software/Hardware (SW / HW) Licensing and Leverage Strategic Sourcing of IT Commodities
- Implement DoD Enterprise-wide IT Asset Management

- **Objective 3: Manage the Implementation of the JIE**
  - *Strategy Element*
    - Drive Implementation of Capabilities to Achieve the JIE

- **Objective 4: Strengthen IT Governance**
  - *Strategy Elements*
    - Improve the Effectiveness of the DoD CIO Executive Board and Associated Governance Bodies
    - Implement the IT Governance Aspects of Digital Government Strategy Milestones 4.2 and 6.3
    - Streamline the Process for Interoperability Certification
    - Improve DoD CIO's Engagement in the Joint Capabilities Integration and Development System (JCIDS), Planning, Programming, Budget, and Execution (PPBE) system, and Defense Acquisition System (DAS)
    - Enhance the Usefulness of IT Portfolio Management Tools

- **Objective 5: Transform IT Financial Management to Implement "End-to-End" Plan-Spend-Performance Decision Making**
  - *Strategy Elements*
    - Conduct IT Compliance Assessments
    - Review Performance of Major Investments
    - Implement an Effective PortfolioStat Process for DoD
    - Establish and Implement Effective IT Portfolio Management / IT Investment Management Policies
    - Establish Accountability and Auditability for Internal Use Software Investments
    - Support Audit Readiness for Financial and Mixed Systems that Impact Financial Reporting

- **Objective 6: Streamline the IT Acquisition Process**
  - *Strategy Element*
    - Support Acquisition Approaches that Result in More Rapid Fielding of IT capabilities

Goal 6: Strengthen Cybersecurity

Intended Outcome: *Mission dependability in the face of a capable cyber adversary.*

- **Objective 1: Establish a Resilient Cyber Defense Posture**
  - *Strategy Elements*
    - Architect a Defensible Information Environment
    - Enhance Security through Cyber Hygiene and Best Practices
    - Strengthen Data Defenses
    - Increase Focus on Industrial Control Systems and Embedded Computing

- Institutionalize Threat-Based Engineering and Acquisition

- **Objective 2: Transform Cyber Defense Operations**
  - *Strategy Elements*
    - Improve Active Cyber Defense Capabilities
    - Mitigate All Phases of Cyber Aggression
    - Ready Forces to Maneuver
    - Employ Unpredictable Defenses
- **Objective 3: Enhance Cyber Situational Awareness**
  - *Strategy Elements*
    - Improve the Cyber Sensing Infrastructure
    - Harness the Power of Big Data Analytics
    - Implement a Multi-Mission Cyber Operational Picture
    - Increase Information Sharing and Cooperation
- **Objective 4: Assure Survivability Against Highly-Sophisticated Cyber Attacks**
  - *Strategy Elements*
    - Assure Survivability of High Priority Mission Areas
    - Prepare for Success Against Large-Scale Cyber Attacks
    - Quickly Regenerate Cyber Capabilities

Goal 7: Forge Partnerships

Intended Outcome: *Positive synergies in processes, technologies, and intellectual capital are mutually beneficial to DoD and its partners.*

- **Objective 1: Establish Clear Roles and Responsibilities with DoD and Interagency Partners on NLCC Support**
  - *Strategy Elements*
    - Specify Roles and Responsibilities for NLCC
- **Objective 2: Enable Information Sharing and Collaborative Agreements with Key Allies and Partners**
  - *Strategy Elements*
    - Oversee Agreements for Sharing Communication Systems and Services
    - Engage with Key Allies and Partners to Improve Interoperability with U.S. by Sharing Information and Collaborating on Information Management (IM) C2, Communication Systems and Related Policy
    - Strengthen the Multi-National Information Sharing Initiative
- **Objective 3: Enhance the DoD Connection Approval Process for Non-DoD Partners**
  - *Strategy Element*
    - Establish Memorandum of Understanding (MOU) and Memorandum of Agreement (MOA) with Other Federal, State, Local and Tribal Partners, As Needed

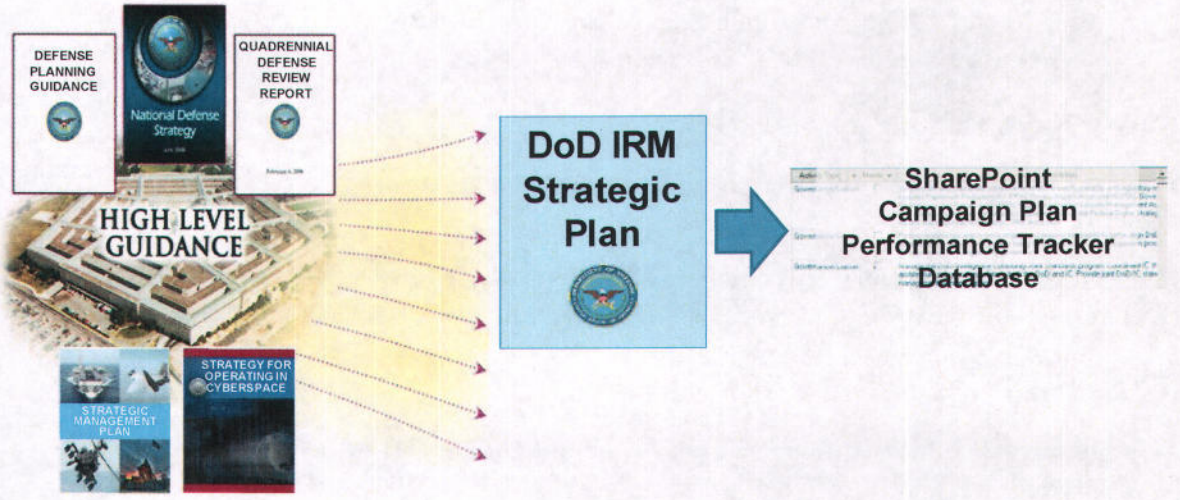
Responding to High Level DoD Guidance (DoD Strategic Goals and Objectives)

Required OMB Content:

- *Identify DoD strategic goals and objectives supported by the IRM strategic plan (AXXA)*
- *Describe how activities of the IRM Strategic Plan and Enterprise Roadmap advance these goals and objectives (AXXB)*

(AXXA) The DoD IRM Strategic Plan v1.0 presents our mission, vision, strategic goals and objectives, which provide the DoD CIO's support of the goals, priorities and objectives found in the National Defense Strategy, the Quadrennial Defense Review (QDR), the Defense Planning Guidance (DPG), and the Strategic Management Plan (SMP), as well as legislative guidance and direction contained in National Defense Authorization Acts (NDAA) and high level strategies such as the Strategy for Operating in Cyberspace.

Figure 1: DoD IRM Support for DoD Strategic Goals and Objectives



2014 DoD Strategic Plan

The 2014 and 2015 DoD Budget Requests establish the Department's Strategic Goals based upon the 2010 QDR. The DoD Strategic Goals are:

- Prevail in today's wars
- Prevent and deter conflict
- Prepare to defeat adversaries and succeed in a wide range of contingencies
- Preserve and enhance the All-Volunteer Force
- Reform the business and support functions of the Defense enterprise

FY2014-2018 Defense Planning Guidance

The FY2014-2018 DPG identifies 11 primary missions that determine and shape the future Joint force. The IRM Strategic Plan goals listed above align and support all of these missions.

The Strategic Management Plan and Annual Performance Plan

The SMP, developed by the Deputy Chief Management Office (DCMO), establishes the Department's management goals for business operations likewise linked to the Department's overarching strategic goals and objectives. This DoD IRM Strategic Plan fully supports the SMP business goal for the DoD CIO to "Build agile and secure information technology capabilities to enhance combat power and decision making while optimizing value." In particular, this DoD IRM Strategic Plan supports all seven key SMP initiatives related to this goal, as illustrated below in Table 1[5]:

1. Enable secure, mobile, and mission-driven access to information across the enterprise.
2. Provide enterprise IT infrastructure and services across DoD.
3. Establish a multi-provider DoD enterprise cloud environment.
4. Advance and evolve IT infrastructure to support mobile devices and promote development and use of DoD mobile and web-enabled applications.
5. Implement improved cybersecurity through continuous monitoring, and global identity and access management
6. Implement changes to IT and cybersecurity workforce management.
7. Provide strategic sourcing of hardware, software, and services.

The DoD IRM Strategic Plan further supports three of DoD's specific strategic objectives from the Department's FY13 Annual Performance Plan (APP):

- DoD Strategic Objective 3.4-1X1: Expand capacity to succeed against adversary states armed with anti-access capabilities and/or nuclear weapons and improve capabilities to conduct effective operations in cyberspace and space.
- DoD Strategic Objective 4.4-2T: Train the Total Defense Workforce with the right competencies.
- DoD Strategic Objective 5.2-2C: Protect critical DoD infrastructure and partner with other critical infrastructure owners in government and the private sector to increase mission assurance.

As with recent DoD CIO campaign planning efforts, the DoD IRM Strategic Plan and the associated DoD CIO Campaign Plan continue to support the Secretary of Defense's memo to the Deputy Secretary of Defense of October 17, 2011 that set the priority for the Department to implement savings—in efficiencies, personnel costs, modernization and procurement reform.

[5] Department of Defense Strategic Management Plan FY 2012 – FY 2013

(AXXB) Table 1 illustrates how each initiative in the FY14-15 SMP is supported by at least one particular goal, objective, and Strategy Element (SE) in the DoD IRM Strategic Plan. The table further illustrates how specific Annual Performance Plan objectives are supported by IRM goals, objectives, and strategy elements.

Table 1: DoD IRM Strategic Goal Alignment to SMP Initiatives and APP Objectives

SMP Initiative / APP Objective	IRM Strategic Plan Goal / Objective / Strategy Element (SE)
Strategic Management Plan Initiatives	
Enable secure, mobile, and mission-driven access to information across the enterprise	**Exploit the Power of Trusted Information Sharing** Objective 1 - Deploy An Authentication Infrastructure To Dynamically Control Authorized User Access To Information • SE 1: Oversee and Guide Implementation of IdAM Infrastructure Capabilities
Provide enterprise IT infrastructure and services across DoD	**Improve Operational Effectiveness and Efficiency Through Superior IT Service Delivery** Objective 1 - Deploy Shared and DoD Enterprise IT Services • SE 2: Implement Federal Shared Services Strategy • SE 3: Develop and Implement New IT Enterprise Services • SE 4: Implement Unified Capabilities • SE 5: Implement IT Service Management • SE 6: Implement Cross-Domain Services Objective 2: Provide a Common Computing Environment • SE 1: Consolidate DoD Data Centers • SE 2: Consolidate IT Infrastructure • SE 3: Establish DoD Enterprise Cloud **Provide a Resilient Communications and Computing Infrastructure** Objective 1 - Improve Communications Networks • SE 1: Improve Tactical Communications Transport Networking • SE 2: Enable a Joint Aerial Layer Networking Capability • SE 3: Provide Satellite Communications Diversity and Resiliency • SE 4: Drive Network Standardization/Modernization • SE 5: Optimize Network Operations • SE 6: Guide Common Configuration Management
Establish a multi-provider DoD enterprise cloud environment	**Improve Operational Effectiveness and Efficiency Through Superior IT Service Delivery** Objective 2 - Provide a Common Computing Environment • SE 3: Establish DoD Enterprise Cloud

SMP Initiative / APP Objective	IRM Strategic Plan Goal / Objective / Strategy Element (SE)
Advance and evolve IT infrastructure to support mobile devices and promote development and use of DoD mobile and web-enabled applications	**Improve Operational Effectiveness and Efficiency Through Superior IT Service Delivery** Objective 3 - Enable Mobile Applications • SE 1: Develop and Implement a Mobile App Store/Mall • SE 2: Develop and Implement Device Native Apps **Provide a Resilient Communications and Computing Infrastructure** Objective 6 - Integrate Commercial Mobile IT Capabilities • SE 1: Evolve the DoD IE Infrastructure to Support Mobile Devices • SE 2: Enable Communications-on-the-Move and Mobile Networking Capabilities
Implement improved cybersecurity through continuous monitoring, and global identity and access management	**Exploit the Power of Trusted Information Sharing** Objective 1 - Deploy An Authentication Infrastructure To Dynamically Control Authorized User Access To Information • SE 1: Oversee and Guide Implementation of IdAM Infrastructure Capabilities **Strengthen Cybersecurity** Objective 1: Establish a Resilient Cyber Defense Posture • SE 1: Architect a Defensible Information Environment Objective 2: Transform Cyber Defense Operations • SE 4: Employ Unpredictable Defenses Objective 3 - Enhance Cyber Situational Awareness • SE 1: Improve the Cyber Sensing Infrastructure • SE 3: Implement a Multi-Mission Cyber Operational Picture
Implement changes to IT and cybersecurity workforce management.	**Evolve the Cyberspace Workforce** Objective 1: Strengthen the Cyberspace Functional Community Workforce • SE 1: Improve Cyberspace Workforce Policy and Planning • SE 2: Eliminate Gaps in DoD High-Risk Mission Critical Occupations / Competencies Objective 2: Strengthen the IT Acquisition Workforce • SE 1: Strengthen IT Acquisition Workforce Competencies • SE 2: Manage, Retool and Implement the IT Program/Project Manager Career Path Objective 3: Enhance Cyberspace Workforce Recruiting, Retention, Education, Training, and Professional Development • SE 1: Modernize IT Workforce Guidance and Training • SE 2: Refine DoD's Cybersecurity Awareness Program
Provide strategic sourcing of hardware, software, and services	**Improve Oversight and Execution of DoD IT Investments** Objective 2 - Manage IT Infrastructure as a Commodity • SE 1: Centralize SW / HW Licensing and Leverage Strategic Sourcing of IT Commodities

SMP Initiative / APP Objective	IRM Strategic Plan Goal / Objective / Strategy Element (SE)
Annual Performance Plan Objectives	
DoD Strategic Objective 3.4-1X1: Expand capacity to succeed against adversary states armed with anti-access capabilities and/or nuclear weapons and improve capabilities to conduct effective operations in cyberspace and space.	**Strengthen Cybersecurity** Objective 1 - Establish a Resilient Cyber Defense Posture • SE 4: Increase Focus on Industrial Control Systems and Embedded Computing Objective 2 – Transform Cyber Defense Operations • SE 1: Improve Active Cyber Defense Capabilities • SE 2: Mitigate All Phases of Cyber Aggression • SE 3: Ready Forces to Maneuver • SE 4: Employ Unpredictable Defenses
DoD Strategic Objective 4.4-2T: Train the Total Defense Workforce with the right competencies.	**Evolve the IT/Cybersecurity Workforce** Objective 3: Enhance IT/Cybersecurity Recruiting, Retention, Education, Training, and Professional Development • SE 1: Modernize IT Workforce Guidance and Training • SE 2: Refine DoD's Cybersecurity Awareness Program
DoD Strategic Objective 5.2-2C: Protect critical DoD infrastructure and partner with other critical infrastructure owners in government and the private sector to increase mission assurance.	**Strengthen Cybersecurity** Objective 1 - Establish a Resilient Cyber Defense Posture • SE 1: Architect a Defensible Information Environment • SE 4: Increase Focus on Industrial Control Systems and Embedded Computing • SE 5: Institutionalize Threat-Based Engineering and Acquisition Objective 2: Transform Cyber Defense Operations • SE 4: Employ Unpredictable Defenses Objective 3 - Enhance Cyber Situational Awareness • SE 1: Improve the Cyber Sensing Infrastructure • SE 4: Increase Information Sharing and Cooperation

FY2012 and FY2013 NDAA

Additionally, the DoD IRM Strategic Plan supports the FY 2012 NDAA Section 2867 requirement for DoD to reduce the resources applied to data servers and data centers through such DoD enterprise efforts as data center consolidation.

The FY2013 NDAA provides additional requirements. Table 2 illustrates how DoD IRM Strategic Plan goals support these requirements.

Table 2: DoD IRM Strategic Plan Goal Support For NDAA Requirements

Section	DoD Requirement	How Supported in DoD IRM Strategic Plan Goals
931	Submit to the congressional defense committees a strategy for implementing the JIE.	**Improve Oversight and Execution of DoD IT Investments** Objective 3 - Manage the Implementation of the JIE
932	Develop a strategy to acquire next-generation host based cyber- security tools and capabilities for the Department of Defense.	**Strengthen Cybersecurity** Objective 3 - Enhance Cyber Situational Awareness
933	Develop and implement a baseline software assurance policy for the entire lifecycle of covered systems.	**Strengthen Cybersecurity** Objective 2 – Transform Cyber Defense Operations
935	Use the available funding and research activities and capabilities of the Community Data Center of Defense Information Systems Agency (DISA) to develop and demonstrate collection, processing, and storage technologies for network flow data.	**Strengthen Cybersecurity** Objective 3 - Enhance Cyber Situational Awareness
936	Conduct an analysis of large-scale software database tools and large-scale software data analysis tools that could be used to meet current and future Department of Defense needs for large-scale data analytics.	**Exploit the Power of Trusted Information Sharing** Objective 3 - Improve Data Management
937	Issue a plan for the inventory of selected software licenses of the Department of Defense, including a comparison of licenses purchased with licenses installed.	**Improve Oversight and Execution of DoD IT Investments** Objective 2 - Manage IT Infrastructure as a Commodity
938	Maintain full visibility and adequate control of its supply chain, including subcontractors, in order to mitigate supply chain exploitation; ...mitigate supply chain risks to its Information Technology (IT) systems that fall outside the scope of National Security Systems.	**Strengthen Cybersecurity** Objective 2 - Transform Cyber Defense Operations
939	Provide to the Committees on Armed Services of the House of Representatives and the Senate quarterly briefings on all offensive and significant defensive military operations in cyberspace carried out by the Department of Defense during the immediately preceding quarter.	**Strengthen Cybersecurity** Objective 1 - Establish a Resilient Cyber Defense Posture Objective 2 - Transform Cyber Defense Operations
941	Establish procedures and criteria that require each cleared defense contractor to report to a component of the Department of Defense designated by the Secretary any successful penetrations of contractor network or information systems.	**Strengthen Cybersecurity** Objective 1 - Establish a Resilient Cyber Defense Posture Objective 2 - Transform Cyber Defense Operations

Section	DoD Requirement	How Supported in DoD IRM Strategic Plan Goals
955	Ensure that the civilian personnel workforce and service contractor workforce of the Department of Defense are appropriately sized to support and execute the National Military Strategy ...develop and begin to execute an efficiencies plan for the civilian personnel workforce and service contractor workforce of the Department of Defense	**Evolve the IT/Cybersecurity Workforce** Objective 1 - Strengthen the IT/Cybersecurity Functional Community Workforce
1079	Provide to the Committees on Armed Services of the Senate and House of Representatives a briefing on the interagency process for coordinating and de-conflicting full-spectrum military cyber operations for the Federal Government.	**Strengthen Cybersecurity** Objective 1 - Establish a Resilient Cyber Defense Posture
1085	All interested parties should be heard when considering a spectrum auction.	**Provide a Resilient Communications and Computing Infrastructure** Objective 7 - Improve Management of Spectrum
2853	Exempt from the applicability of this section research, development, test, and evaluation programs that use authorization of appropriations for the High Performance Computing Modernization Program if the DoD CIO determines that the exemption is in the best interest of national security.	Action is Complete

The preceding Goals section of the IRM Strategic Plan addresses each of these requirements, as indicated by the right-hand column in the table above, with details in the Objectives and Strategy elements within the Goals section.

Key DoD Initiatives and Technologies

Information technology provides the foundation for addressing the information needs of every warfighting, business, and intelligence mission within DoD. IT not only drives modern Warfighter systems, but also links individuals and systems via networks that enable rapid information sharing and command and control. However, if the Department does not take action, then costly, outdated, and stove-piped IT capabilities will continue to stress DoD IT operations and limit interoperability and information sharing across systems. To continue to maintain an information advantage over our adversaries, DoD needs to continually incorporate new commercial technologies and approaches (such as shared services) and increase the pace of fielding technically advanced capabilities to Warfighters. Consequently, DoD's IRM strategy focuses on requirements to improve:

1. Mission Effectiveness: The necessary DoD enterprise infrastructure services to support systems and processes without building separate infrastructure,
2. Cybersecurity: Secure mission-driven access to information and IT services enabled across the DoD enterprise, and
3. Efficiencies: Provide the required IT infrastructure at lower cost through economies of scale, elimination of duplicative services and products, streamlined acquisition, and better use of industry best practices.

The JIE is the primary enabler of this strategy. The intent of the JIE is to provide a unified, reliable, timely, effective, and agile DoD-wide information environment. It is a technical capability that supports DoD's human capital by bringing to bear the power of the DoD IE across the strategic, operational, and tactical levels. JIE users include the Military Departments, Joint Forces, and non-DoD mission partners across the full spectrum of operations at all echelons, and in all operational environments. The JIE will help users achieve full spectrum warfighting superiority, improved mission effectiveness, and increased information security. The JIE encompasses most of the key initiatives for the DoD CIO, including network standardization and data center consolidation.

A critical aspect of the JIE is network standardization, which is achieved through a standardized architecture and SSA that will improve how DoD operates and secures networks on a global level. Users and systems will be able to trust their connection from end to end with the assurance that their activity will not be compromised. Today's environment has 15,000 different networks that are managed to different levels of proficiency.[6] SSA will enable cyberspace operators at every level to see the status of their networks for operations and security and enable commonality in how cyberspace threats are countered. We will know who is operating on our networks, what they are doing and be able to attribute their actions with a high degree of

[6] ITESR, signed 10/5/2011, version 1.0

confidence. Complexity for a synchronized cyber response will be minimized, operational efficiencies will be maximized, and risk will be reduced.

The DoD's IRM strategy relies upon DoD Component contributions to provide innovations that lead to a richer, more satisfying, and cost effective information sharing environment. Component innovation will spring from both CIO-outlined initiatives as well as Component-specific implementations of tools and techniques. Component-developed projects can be vetted for large scale use and promulgated throughout the DoD enterprise. This relationship supports a collaborative approach to exploring and adopting new tools and techniques to keep pace with rapid technological advancements. The Department's approach will be to assess and evaluate beneficial technologies, tools, techniques, procedures, etc. for possible incorporation into the JIE, no matter what the source.

The initiatives highlighted within this DoD IRM Strategic Plan help ensure the DoD CIO is working towards achieving its strategic goals and objectives for managing information resources (including the information itself and related resources, such as personnel, equipment, funds, and information technology) to accomplish agency missions. The intent of IRM is to provide the policy and processes to analyze, select, control, and evaluate those IT investments.

Some of the DoD CIO's key initiatives and technologies currently include:

Enhanced Command, Control, Communications and Computers (C4) Infrastructure (Asia Pacific Rebalancing)

To support the President's and SecDef's Strategic Guidance to rebalance emphasis towards the Asia-Pacific region, the DoD CIO developed and is executing a program of action to improve C4 systems in this area of operation (ref: DoD CIO C4 Strategy Memorandum, 30 Jul 2012). This combined Combatant Command, Service, and Agency (C/S/A) effort involves actions to improve coalition partner information sharing, strengthen existing C4 capabilities in the region, and add new capabilities based on lessons learned from recent operations in the Middle East. Specific actions include increasing capacity and redundancy for Pacific satellite communications gateways, improving resiliency/throughput of existing communications nodes, adding emergency failover capabilities to support critical communications, enhancing cybersecurity/situational awareness, building and improving coalition network capabilities, and implementing a common JIE to improve network effectiveness, efficiency and security in the Pacific theater.

Network Standardization/Optimization

The overarching concept of the JIE is to develop and engineer a standardized network architecture with enduring flexibility to support existing and future capabilities identified by Components and other future Department programs. As stated in one of the JIE guiding principles, common technical standards and processes are the default; uniqueness may be allowed only when essential for mission success. One aspect of network standardization and

optimization is to consolidate duplicative and overlapping networks through elimination of legacy circuit-based capabilities and migrate to converged IP technologies that enable the development of a joint information environment. Currently, operating and securing Service-specific networks is problematic. The planned standardization approach will extend beyond networks to identity and access management processes, data centers, mission and business applications, Commercial Off-The-Shelf (COTS) hardware and software, and IT procurement practices, all of which will enhance efficiency, effectiveness, and security.

Data Center Consolidation/Application Virtualization

A central aspect of the JIE vision is consolidating the number of DoD data centers. Consolidation of data centers, operations centers and help desks will enable users and systems to have timely and secure access to the data and information resource services needed to accomplish their assigned missions, regardless of their location.

The DoD has been engaged in data center consolidation for many years through individual DoD Component activities (e.g., Navy Marine Corps Intranet (NMCI)) and broader Department efforts (e.g., Defense Enterprise Computing Center (DECC)). In 2010, the FDCCI brought data center consolidation to the forefront as a principal lever to achieve enhanced capability delivery, improved cybersecurity, and efficiencies (savings).

Through extensive data collection and discovery efforts, the Department has compiled a global inventory of its data centers based on OMB's broad definition of a data center that includes single servers and storage devices. The DoD has established four classes of data centers to assist in the development and execution of our Data Center Consolidation (DCC) strategy. These four types of data centers are:

- Core Data Center (CDC) – delivers DoD Information Enterprise services and provides primary migration point for systems and applications;
- Installation Processing Node (IPN) – provides local services to DoD installations and hosting systems not suited for CDCs;
- Special Purpose Processing Node (SPPN) – provides computing and storage for fixed infrastructure or facilities (e.g., test ranges, labs, medical diagnostic equipment, machine shops, etc.);
- Tactical/Mobile Processing Node (TPN) – provides support to the deployed Warfighter at the tactical edge.

This hierarchy and the data center architecture it supports are presented in the DoD Core Data Center Reference Architecture dated October 2012. By providing the foundation for the DoD's DCC efforts, this architecture is a principal enabler of the JIE and the instantiation of the Department's cloud computing capability.

To date, nearly 90% of DoD data centers have an identified end-state based on either one of the four data center types CDC, IPN, SPPN, TPN) or an end-state of "Closed." Currently, nearly 50% of all DoD data centers are planned to close within the Future Years Defense Plan (FYDP) with the remaining data centers transforming and conforming to JIE standards.

DoD Enterprise Cloud

Cloud computing is a critical component of the Department's IT modernization, Joint Information Environment, Federal Data Center Consolidation Initiative, and Department wide IT efficiency initiatives. The DoD CIO's key objective is to drive the delivery of an enterprise cloud environment that will reduce costs, minimize risk, and enhance mission effectiveness. DoD CIO is committed to accelerating the adoption of cloud computing within the Department and has determined that commercial cloud computing services will be an integral component of the DoD Enterprise Cloud.

We are diligently evaluating commercial cloud services in areas such as information assurance, cybersecurity, continuity of operations, and resilience given the nature of the Department's mission and the risk to our networks and National security. We have examined and understand the need to balance risk and cost to the Department when utilizing commercial cloud and have published guidance to help DoD cloud consumers identify the appropriate data protection and needed cybersecurity mechanisms when selecting and using commercial cloud. Before a cloud provider is allowed to connect to the DoD Information Network (DODIN) we will require them to obtain a DoD Provisional Authorization by completing the Federal Risk Authorization and Management Program (FedRAMP) authorization process and demonstrating adherence to the recently developed DoD Cloud Computing Security Requirements Guide (the Guide). The Guide supplements FedRAMP and details security requirements needed to minimize risks to the DODIN. It provides clear guidance to both Cloud Service Providers and DoD Cloud Customers by describing the cradle-to-grave process they must follow in order to move DoD computing rapidly and securely into commercial cloud infrastructure.

DISA is developing a Cloud Access Point (CAP) to offer a means to connect commercial cloud service providers (CSPs) to our networks in order to monitor, defend, and protect our networks and information. To this end, DISA is leveraging lessons learned from the Navy's point-to-point implementation with a major commercial cloud service provider, and other Components' piloting efforts.

DoD CIO will ensure that Components will only use cloud services that have: a DoD Provisional Authorization; an Authority to Operate (ATO) by their Authorizing Official; a connection through a DoD CIO approved CAP; and a Component CIO approved business case analysis.

Done correctly, cloud computing represents a significant opportunity to improve the performance, efficiency and security of DoD IT. To achieve this vision, the DoD CIO continues

to work with other senior leaders at the Pentagon to ensure that we are delivering the right policies and guidance to drive the appropriate adoption of cloud computing.

Enterprise Cross-Domain Services

The DoD Intelligence Community (IC) and other U.S. Government entities envision a future in which the need for secure information sharing across domains of different classifications and sensitivity levels will continue to increase and in which Enterprise Cross Domain (ECD) services will be the standard. Cross domain products and services are provided by three main methods. These are:

1. "Bring the data to the user" involves moving data from one domain to another. When importing data from a less trusted environment, the cross domain capability filters the data and the data structures to find and remove malware. If the data is being exported from a more trusted environment, a sanitization process occurs to ensure data release restrictions are properly followed.

2. "Bring the user to the data" involves authenticating and authorizing users' access to data typically stored in large databases. The cross domain technology mediates the user's rights against the labels or tags applied to the data itself by the data owner, consistent with need-to-know criteria. The data owner is responsible for establishing the need-to-know criteria.

3. "Multi-level" cross domain techniques are typically machine-to-machine transfers where the blend of filtering, sanitization and machine authorizations is brought to bear. Most of the cross domain instances involve large datasets (imagery files, etc.). This cross domain method is highly automated as compared to the previous two user-centric models.

The migration of cross domain solutions (individual point-to-point) products towards Enterprise Cross Domain services meets many of the DoD IRM goals. Provisioning ECD as a security-critical service leads to more effectiveness across the DoD, IC and Civil Agencies (all partners in information sharing activities) by consolidating the technologies, operations, management and cybersecurity associated with information accessibility.

While several key areas have been addressed recently, plans are to align key areas in order to provide secure and assured DoD enterprise information resources and ECD critical capabilities that will rapidly provide secure information sharing amongst a diverse set of partners.

Strengthened Cybersecurity

Cybersecurity is one of the highest priorities of the Department. The primary cybersecurity goal of the DoD CIO is ensuring that essential DoD missions are dependable and resilient in the face of cyberspace warfare by a capable adversary. This focus on mission assurance, rather than on computer or system security, is one of the primary changes in the Department's cybersecurity approach. Another change is the focus in JIE of giving certain operational commanders more

freedom to take operational cybersecurity risks by using "risk zones" in the design of the JIE computing and networks; these zones help keep the risks assumed by a particular mission from spilling over into other missions. This is also a significant change from today's DoD networks, which impose more operational constraints on commanders. Other primary cybersecurity goals include improved safe sharing with whatever partners a mission requires, and a continued need to keep a secret. Through refinement of the JIE concept, the DoD CIO has concluded that all of these cybersecurity goals can be achieved, and the Department will have better joint warfighting decision support, better operational and acquisition agility, and better efficiency.

Responsibility for defining and executing the Department's cybersecurity program spans many organizations in DoD, particularly the U.S. Cyber Command (USCYBERCOM). DoD CIO also works closely with the Military Departments, nine Defense Agencies, and the elements of the OSD to ensure cybersecurity issues are being addressed.

Given the complexity of the cybersecurity challenge, and of DoD's Information Enterprise, there are a wide range of technical and operational efforts aimed at achieving the above cybersecurity goals. Initiatives in support of the dependability and secrecy goals include efforts to remove vulnerability, to shield latent vulnerabilities by layering defenses, and to ensure an understanding of where vulnerabilities still exist. In spite of best efforts to harden DoD systems, an adversary may still succeed, so there are also a variety of efforts to contain, dampen, detect, diagnose, and react to successful or partially successful cyberspace intrusions and attacks.

In the last year, the DoD CIO has focused on the development of the JIE SSA, a unifying, joint cybersecurity approach for the design of the JIE. Although many of the DoD's cybersecurity initiatives are common across all DoD organizations, each DoD Component has had the ability to make important decisions about how to design computing and networks and about how to structure cyber defenses. This has led to several challenges, such as diversity in the cybersecurity protections of the DoD that does not provide a common level of protection for joint missions (because the IT for these missions is designed and operated by many organizations), and sometimes interferes with the collaborative attack detection, diagnosis, and reaction so necessary in a complex organization like DoD. Finally, the challenge caused by this diversity can interfere with a Joint commander's ability to share information with external mission partners.

To solve these problems, the SSA provides for a common approach to the structure and defense of computing and the networks across all DoD organizations. For example, the SSA describes how core DoD data centers and the servers they contain must be configured; which cybersecurity defenses are required on these computers; which cybersecurity "firebreaks" are necessary as part the internal networks of the data center; how remote management and automation of the data center is to be structured and secured; and which cyberspace-attack detection, diagnosis, and reaction capabilities the data center and the remote management system must have. As another example, the SSA defines the structure of the computing and networks on a typical military base. For example, all computer servers that must be located close to end-users (such as print servers)

will be located in an installation processing node data center. The computers in this node must be configured and managed to DoD-wide cybersecurity standards and use DoD standard defense and situational awareness tools, and the installation processing node must be outfitted with perimeter defenses that can be configured to meet DoD-wide policies. All information about this computing node and its defenses must be shared throughout the joint DoD cyber defense operational structures. A final example is that the SSA requires that the cyberspace identity credentials from the DoD Public Key Infrastructure (PKI) be used in every access to information in the JIE so as to drive anonymity out of the DoD networks, and it defines how directories that are used in access control decisions must be structured to strongly inhibit a cyberspace adversary's ability to move laterally inside the Department's networks.

This engineering of the cybersecurity approach "end-to-end" will significantly improve DoD's ability to resist cyberspace attacks; to dampen the spread of successful attacks; and to detect, diagnose, and react to attacks in ways that are optimized for joint missions. Owing to the standardization and cyberspace data sharing of JIE, cyberspace defenders will have broad visibility into the computing and networks, and via secure remote management and automation, they will be able to much more quickly construct and execute defensive actions. In addition, the SSA-defined risk containment zones in the computing and the network will enable Joint commanders to better contain cyberspace risk to missions while sharing as broadly with external partners as a mission requires. It will also make development of new decision support capabilities simpler and easier since many program offices will not need to worry about most cybersecurity protections, but will instead be able to build software applications on top of the standard protections and situational awareness capabilities provided by JIE.

PKI

The DoD PKI cyberspace identity credential that is stored on the DoD Common Access Card is used by every DoD user on the unclassified networks. On the Department's secret networks, similar cyberspace identity credentials are being deployed. This is a central part of efforts to drive anonymity out of the networks, and to drive up the accountability required for a successful insider threat management program. To date, more than 300,000 smart cards with these PKI credentials for secret networks have been issued and implementation efforts have begun for cryptographic logon for accounts using these credentials.

The U.S. Government's secret networks are interconnected to improve interagency sharing of mission essential information. Standardization of the defenses of all of these networks is essential to the security of every agency, including DoD. PKI cyberspace identity credentials will enable other agencies to more quickly drive out anonymity on their secret networks, and to drive up accountability in a cross-organization way via the use of a standard cyberspace identity credential. DoD's PKI Common Service Provider (CSP) issues NSS PKI credentials to DoD personnel and to other Federal agencies' personnel via an OMB-coordinated, shared fee for service cost model. The NSS PKI credentials issued by the DoD PKI CSP are only for use on the

Secret network fabric. Use of these credentials will not only help improve accountability for information access, but as DoD works with the rest of the U.S. Government, will make interagency sharing safer and easier.

IdAM

DoD requires a mission-enabling IdAM capability over the next 3-5 years that will allow "Person and non-person entities secure access to all authorized DoD resources, anywhere, at any time." The required IdAM capability will ensure access control is dynamic (automatic and data-driven); person and non-person entities can be discovered (e.g., via White, Blue, and Yellow pages); activity monitoring is strengthened; person and non-person entity data are complete, trusted, accurate, and accessible; collaboration and interoperability are enabled; and IdAM is institutionalized in the form of established policies and repeatable standards. These objectives increase Warfighter effectiveness by enabling secure discovery, sharing, and use of resources and information among mission partners, increase security by tying identities to accountable actions, and achieve efficiencies by automating existing manual access control mechanisms across the DoD enterprise.

Supply Chain Risk Management

In other areas of cybersecurity, rapid uptake of advanced commercial technology remains a key DoD advantage. While globally sourced technology provides innumerable benefits to the Department, it also provides foreign sources with increased opportunity to compromise the supply chain by inserting malware into technology in order to access or alter data, and intercept or deny communications. In response to these risks, DoD is institutionalizing the Trusted Defense Systems / Supply Chain Risk Management strategies described in the Report on Trusted Defense Systems delivered to the Congress in January 2010. The Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) and the DoD CIO jointly issued DoD policy in November 2012 that makes permanent the Department's policies to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or components. The DoD CIO office and the office of the USD(AT&L) oversee implementation of this policy and work closely with the Military Departments and nine Defense Agencies, including DISA, the National Security Agency (NSA), the Defense Intelligence Agency (DIA), and the Defense Logistics Agency (DLA), to achieve full operating capability for the Department.

In addition, representatives from the office of the DoD CIO and the Department of Homeland Security (DHS) worked with the Committee on National Security Systems (CNSS) to develop CNSS Directive 505 - Supply Chain Risk Management, which serves as the supply chain policy that applies to all national security systems within the Federal Government. DoD is partnering with other departments and agencies to explore approaches to managing supply chain risk within critical infrastructures, which are critical to executing DoD missions.

The Defense Industrial Base Cybersecurity/Information Assurance Program

DoD operates a successful public/private cybersecurity information sharing program that is a model for other government/industry cybersecurity efforts: DoD's Defense Industrial Base (DIB) Cybersecurity and IA (CS/IA) Program. This program offers a model standard for government/industry voluntary partnerships on cybersecurity. The program provides two-way cybersecurity information sharing to include classified threat information sharing by the government, with voluntary sharing of incident data by industry, as well as sharing of mitigation and remediation strategies, digital forensic analysis, and cyberspace intrusion damage assessments. As an example, DoD provides fast analysis of malicious software reported by industry and quickly shares with the DIB CS/IA participants, and with the rest of the Federal Government, machine readable indicators of the attack that can very quickly be deployed to protect others against new and emerging threats detected by any of the participating companies.

While threats cannot be eliminated, the DIB CS/IA program enhances each DIB participant's capabilities to mitigate the risk, thereby further safeguarding DoD information that resides on, or that transits, DIB unclassified networks. Building on this successful model, DoD partnered with DHS to put in place a means of using higher classified information to protect the networks of participating companies. Under the DIB Enhanced Cybersecurity Services program, the U.S. Government provides highly classified cybersecurity threat information either directly to a DIB company or to the DIB company's CSP. This sensitive, government-furnished information enables these DIB companies, or the CSPs on behalf of their DIB customers, to counter additional types of malicious cyberspace activity. The CSPs provide the protections as a commercial fee-for-service offering; the government is not involved in the financial aspects of the transaction between a CSP and the participating DIB company. DoD is the government point of contact for the participating DIB companies, through the DoD's DIB CS/IA Program. DHS is the government point of contact for participating CSPs, under the umbrella of DHS's Joint Cybersecurity Services Program, a broader effort to protect U.S. critical infrastructure.

Future of Cybersecurity

Transforming cyberspace defenses and regaining the advantage against cyberspace adversaries will require new strategic imperatives, such as shifting from reactive to more pro-active cyber defense operations, and focusing a greater portion of cyber defense activities on adversary activities and intent. Currently, the approach to cyber defense is based primarily on policy compliance, hardening configurations, and patching vulnerabilities, which are necessary but not sufficient. As the DoD focuses on cyber defenses driven by intelligence about the potential adversary, this shift will enable improvements to detect, protect, and respond to the threat's quickly changing cyber tactics. The term "active cyber defense" describes this new approach, which is DoD's synchronized real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It operates at network speed by sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. Adversaries

will discover they cannot single out and attack local units without bringing to bear broader DoD support from intelligence and cybersecurity forces. Active cyber defense is a transformational capability in an early operational stage. DoD will refine and evolve its capabilities by leveraging advances in all aspects of cybersecurity operations and integrating national, regional, and organizational cyber defenses into a coherent active cyber defense framework.

Improved Senior Leader Communications

The Deputy Secretary of Defense recently established a Joint Systems Engineering and Integration Office under DoD CIO direction, through the Director of DISA, to manage issues across Senior Leader Communications/Nuclear Command Control and Communications/ Continuity Communications. This approach will ensure a focused end-to-end integration of requirements, configuration management, assessments, and architecture in these areas.

Related and complementary to this function, the DoD CIO co-chairs, along with a DHS representative, the National Security/Emergency Preparedness (NS/EP) Communications Executive Committee. This is a forum with members from the Departments of State, Defense, Justice, Commerce and Homeland Security; the Office of the Director of National Intelligence; the General Services Administration (GSA); and the Federal Communications Commission. The forum is responsible for ensuring the Federal Government has the ability to communicate at all times and under all circumstances to carry out its most critical and time sensitive missions, and for recommending policy and advising the President of the United States on NS/EP communications issues.

Improved Management of Spectrum

Management of the electromagnetic spectrum has become increasingly important to the Department's missions, consumers, and the economy of the Nation. The use of the electromagnetic spectrum continues to be a critical enabler of our warfighting capabilities and cyberspace operations. Defense leadership is cognizant and sensitive to the unprecedented spectrum demands resulting from the Department's increasing reliance on spectrum-dependent technologies and the rapid modernization of commercial mobile devices. Fully recognizing the linkages between national security and economic prosperity, the Department is investing in technologies and capabilities aimed at more efficient uses and management of spectrum, and for increased interoperability with our coalition partners and with Federal, State, and Commercial entities. Future spectrum legislative proposals will seek to achieve a balance between expanding wireless and broadband capabilities for the nation and the need for spectrum access to support warfighting capabilities in support of our national security.

DoD is already proactively working with the National Telecommunications and Information Administration (NTIA), other Federal partners, and industry to methodically evaluate spectrum bands, through established deliberate processes. One example of DoD's extensive efforts, actively working with industry, was to assess the feasibility of sharing the 1755-1850 MHz band

through the NTIA established working groups under the Commerce Spectrum Management Advisory Committee (CSMAC). The CSMAC working groups' effort is an example of unprecedented collaboration between DoD and commercial industry to assess highly complex technical issues with a goal of ensuring practical and balanced spectrum repurposing decisions that are technically sound and operationally viable from a mission perspective.

DoD Radio and Communication Security (COMSEC) Modernization

The DoD CIO is working with the Military Departments to capitalize on opportunities to shift from legacy tactical radio and COMSEC technologies, ensuring the modernization of tactical radios and associated secure communications capabilities in a timely and cost-and-capability-effective manner. The DoD CIO is working to guide military service plans for radio and waveform improvements, synchronized with secure communications modernization. DoD CIO actions will inform proactive investment planning to achieve a cost-effective migration to preferred radio characteristics. The DoD CIO has established a framework of objectives, metrics and oversight to measure progress and facilitate visibility and coordination of Service actions.

Commercial Integration

As mentioned in the DoD Enterprise Cloud section above, the Department is working to broaden its use of commercial solutions. The DoD Mobile Device Strategy, published on June 8, 2012, identified IT goals and objectives to capitalize on the full potential of mobile devices in the Department. The strategy focuses on the networking infrastructure to support wireless devices, mobile devices, and mobile applications, and a framework to ensure that the Department's use of commercial mobile devices is reliable, secure, and flexible enough to keep up with fast-changing technology.

As follow-on to that strategy, the DoD CIO issued the DoD Commercial Mobile Device Implementation Plan on February 15, 2013. The implementation plan updates the Mobile Device Strategy and establishes a framework to equip the Department's 600,000 mobile-device users with secure-classified and protected-unclassified mobile solutions that leverage commercial off-the-shelf products, encourage the development and use of mobile applications to improve functionality, decrease costs, and enable increased personal productivity. The plan orchestrates a series of operational pilots from across DoD Components that will incorporate lessons learned, ensure interoperability, refine technical requirements, influence commercial standards, and create operational efficiencies for DoD mobile users. The DoD Mobile Device Strategy and Implementation Plan aim to align the various mobile devices, pilots and initiatives across DoD under a common security and cost framework that aligns with efforts in the JIE. This is not simply about embracing the newest technology – it is about keeping the Department's workforce relevant in an era when information accessibility and cybersecurity play a critical role in mission success.

Key partners in these efforts are DISA and NSA, who, working together with industry, have developed security configuration baselines for several of the major smart phone technologies and are working on more. The Military Departments are also actively involved in these efforts and will be responsible for helping develop mobility applications. The DoD CIO actively participates in the Federal CIO's Digital Government Strategy initiatives, including commercial mobile capabilities integration across the Federal Government. DoD CIO coordinates with OMB, the National Institute for Standards and Technology (NIST), and CNSS on national security guidance for commercial mobile platforms in accordance with their FISMA and Executive roles and responsibilities. DoD CIO coordinates with the GSA on its Federal Strategic Sourcing Initiative (FSSI) for Mobile Lifecycle & Expense Management regarding consolidated wireless service contracts, Mobile Device Management (MDM), and Telecommunications Expense Management (TEM) services. DoD CIO continues to coordinate with its Federal partners on the next phase of the Digital Government Strategy, especially with the Information Security and Identity Management Committee's (ISIMC) Mobile Technology Tiger Team on IdAM, mobile application vetting and development, continuous monitoring, and data sharing.

DISA and its partners achieved version 1.0 of the unclassified mobility capability on January 31, 2014 with iOS support and Release 2.0 on May 9, 2014 with Android support. DISA and its partners are working to create a secure adaptive mobile environment necessary to incorporate the steady advancement of technology, including application development, changing security architecture requirements, and continuous enhancement of equipment.

Additional discussion of DoD's mobility efforts is found in the Improving Services to Customers and Commodity IT and Shared Services sections of this plan.

DoD Enterprise IT Services

The DoD Information Enterprise will provide a suite of online tools as IT services to help DoD personnel accomplish their missions. The suite of IT services will adapt over time to meet evolving needs and expectations and will leverage the capabilities of current available technologies. IT services will be delivered at the DoD level both to achieve cost efficiency and mission effectiveness.

DoD Enterprise IT services provide efficiency by reducing redundancy in duplicative IT investments, and operations cost. Consolidated delivery of capabilities through common IT services reduces complexity, which provides both first-order effects associated with elimination of unnecessary IT, but also second-order effects such as simplified business processes enabled by those common IT services.

The DoD is focusing on the acquisition of IT services with clear delineation of service provider responsibilities for system operations and customer satisfaction. Accordingly, the DoD CIO is working to establish governance mechanisms to manage the overall DoD portfolio of enterprise

IT services, including the identification and oversight of DoD enterprise IT service providers and establishment of common processes for service delivery and service management.

Within DoD's JIE framework, a service provider is a Military Department, Agency, or other organization that provides some kind of communications, storage, or processing service, or any combination of the three, to mutually understood levels of service. Some of these operational capabilities may be externally provided by non-Military Department or Agency entities outside of the JIE operational construct. Examples from the current DoD IT environment are: DISA's role in providing DISN transport services and DoD enterprise email and the DISA Defense Enterprise Computing Center's role in providing these and other DoD enterprise IT services. The JIE construct may also allow IT services to be commercially provided.

Within JIE, DoD enterprise IT services will be provisioned in the most efficient manner that meets availability and quality of service requirements. Critical IT services with high real-time management requirements may need to be distributed. However, by keeping the number of service points to a minimum, both operational effectiveness and efficiencies will be gained.

Unified Capabilities

Technology is driving the Department toward IP-based Unified Capabilities (UC) (defined in DoD Instruction 8100.04 as "the integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the Warfighter and business communities") services. For example, the commercial sector is rapidly phasing out the manufacture and support of voice-related legacy equipment and shifting to all IP-based technologies, with end of life expected by 2016.

To take advantage of the expanding IP-based service offerings of commercially driven off-the-shelf, software-based UC, DoD developed an end-state vision to migrate to a service-rich set of capabilities. In October 2011 the DoD CIO signed the Unified Capabilities Master Plan, which defines the DoD migration strategy toward converged, net-centric, IP-based voice, video, and/or data services.

As a first step to full implementation of UC, the Department has developed an architecture-based enterprise-wide plan to provide global voice services provisioned over IP-based networks. This Enterprise VOIP capability will provide DoD enterprise voice service to the Department's 2.7 million users at over 1,600 locations worldwide, while creating a multi-purpose infrastructure for the subsequent implementation of other UC services (i.e., video, chat, data, collaboration, and unified messaging).

In addition to enhancing mission effectiveness via the benefits of converged voice, video, and data services, the Department will realize significant reduction in operations and maintenance costs, avoid procurement cost for replacement of the legacy circuit switches that are at

commercial end-of-life, and leverage DoD's substantial aggregate buying power for additional cost savings.

Financial Improvement Audit Readiness (FIAR) Initiative

The Department's methodology for achieving improved financial information and auditability has evolved and has been refined since the FIAR Plan was first issued in 2005. The FIAR Plan priorities were established in August 2009 and require the Components to first focus on improving processes, controls, and systems supporting information most often used to manage the Department. This is the starting point for achieving the goal of obtaining auditable financial statements, beginning with the Statement of Budgetary Resources. To achieve these objectives, the FIAR priorities are:

- Budgetary information
- Mission critical asset information
- Auditability of all financial statements by 2017

The Component Financial Improvement Plans (FIPs), when summarized collectively, compose the Department's FIAR Plan. The DoD Components' FIPs are prepared and executed in accordance with FIAR Guidance issued by the Office of the Under Secretary of Defense (Comptroller) (OUSD(C)). The FIAR Guidance provides the strategy and standard methodology, as well as the step-by-step approach for discovery and evaluation; documenting, testing, and strengthening controls; and achieving an audit ready systems environment.

Existing and future systems will need to satisfy joint general and application level control requirements identified in the FIAR Guidance and the Federal Information System Controls Audit Manual. In support of this requirement during FY 14, the DoD CIO updated DoD Instruction (DoDI) 8510.01 (Risk Management Framework for DoD Information Technology) and OUSD(C) and the DoD CIO will jointly author and distribute supplemental guidance to address the FIAR requirements for relevant systems. The supplemental financial system implementation guidance will be published by the Comptroller and also be posted on the DoD CIO's Knowledge Services website. Furthermore, the DoD CIO and Comptroller will continue to review existing policy and procedures and incorporate additional FIAR requirements as needed.

In addition, Departmental investments made in Internal Use Software, purchased (COTS) or internally developed, will need to be accounted for in a manner that addresses financial statement auditability requirements. Accordingly, the Department's office of the CIO will develop and implement policies and procedures to meet the auditability requirements for Internal Use Software identified in the FIAR Guidance including:

- Financial Statement Assertions
- Key Risks of Material Misstatement
- Financial Reporting Objectives

- Key Supporting Documents
- Outcomes Demonstrating Audit Readiness
- Audit Readiness Testing Procedures

Relationship with DoD Partners

The DoD CIO relies on close relationships with other DoD and OSD Components to realize the DoD CIO Vision and Mission, including the Military Departments, USD(AT&L), Under Secretary of Defense for Policy (USD(P)), Under Secretary of Defense for Intelligence, USD(C), Cost Assessment and Program Evaluation (CAPE), DCMO, DISA, NSA, USCYBERCOM, and the Joint Staff. The DoD CIO works with members of these organizations to develop and implement strategies to strengthen and improve the operational effectiveness, efficiency, and security of the Department's networks and information sharing infrastructure.

The DoD CIO's relationship with DISA is particularly important. DoD CIO and DISA senior leadership have been working together with increasing frequency, to review critical areas of common concern and to discuss ways to enhance the working relationship between the organizations. In addition, DoD CIO and DISA planning teams meet and coordinate as required to bring the goals, priorities, actions, and tasks in their respective campaign plans into greater alignment—especially by identifying potential gaps or areas that may need greater coordination.

Relationship with Federal Partners

1. Federal CIO Council

The CIO Council is the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal information resources. The CIO Council is one element of an interagency support structure established to achieve information resource management objectives delineated in legislation including the E-Government Act of 2002, Government Paperwork Elimination Act, Paperwork Reduction Act, Government Performance and Results Act, and the Information Technology Management Reform Act of 1996.

The Chair of the CIO Council is the Deputy Director for Management for the Office of Management and Budget and the Vice Chair is elected by the CIO Council from its membership. Membership on the Council comprises CIOs (to include DoD CIO) and Deputy CIOs from 28 Federal executive Agencies. Additional members of the Council include liaisons from other Federal level councils and committees.

2. National Security Emergency Preparedness

The Federal Government must have the ability to communicate at all times and under all circumstances to carry out its most critical and time sensitive missions. Survivable, resilient, enduring, and effective communications, both domestic and international, are essential to enable the executive branch to communicate within itself and with: the legislative and judicial branches; State, local, territorial, and tribal governments; private sector entities; and the public, allies, and other nations. Such communications must be possible under all circumstances to ensure national security, effectively manage emergencies, and improve national resilience. The views of all levels of government, the private and nonprofit sectors, and the public must inform the development of NS/EP communications policies, programs, and capabilities.

Specific Department and Agency responsibilities for National Security Emergency Preparedness are discussed below.

The Secretary of Defense shall:

(a) oversee the development, testing, implementation, and sustainment of NS/EP communications that are directly responsive to the national security needs of the President, Vice President, and senior national leadership, including: communications with or among the President, Vice President, White House staff, heads of state and government, and Nuclear Command and Control leadership; Continuity of Government communications; and communications among the executive, judicial, and legislative branches to support Enduring Constitutional Government;

(b) incorporate, integrate, and ensure interoperability and the optimal combination of hardness, redundancy, mobility, connectivity, interoperability, restorability, and security to obtain, to the

maximum extent practicable, the survivability of NS/EP communications under all circumstances, including conditions of crisis or emergency;

(c) provide to the Executive Committee the technical support necessary to develop and maintain plans adequate to provide for the security and protection of NS/EP communications; and

(d) provide, operate, and maintain communication services and facilities adequate to execute responsibilities consistent with Executive Order 12333 of December 4, 1981, as amended.

The DoD CIO is the co-chair along with DHS.

3. Senior Information Sharing and Safeguarding Steering Committee

Established by Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," the Senior Information Sharing and Safeguarding Steering Committee will exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.

The Steering Committee is co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff. Members of the committee are officers of the United States as designated by the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration (NARA), as well as such additional agencies as the co-chairs of the Steering Committee may designate. The DoD CIO represents DoD in the Senior Information Sharing and Safeguarding Steering Committee as a voting member of the committee.

DoD (DoD CIO) along with NSA execute jointly the additional responsibilities of the Executive Agent for Safeguarding Classified Information on Computer Networks (the "Executive Agent") as per Executive Order 13587. The Executive Agent's responsibilities, in addition to those existing authorities of the Executive Agent and National Manager for NSS specified by National Security Directive-42, include the following:

(a) developing effective technical safeguarding policies and standards in coordination with the CNSS;

(b) referring to the Steering Committee for resolution any unresolved issues delaying the Executive Agent's timely development and issuance of technical policies and standards;

(c) reporting to the Steering Committee on the work of CNSS, including recommendations to improve the timeliness and effectiveness of that work; and

(d) conducting independent assessments of agency compliance with established safeguarding policies and standards, and reporting the results of such assessments to the Steering Committee.

4. Committee on National Security Systems

The CNSS, which is subordinate to the Senior Information Sharing and Safeguarding Steering Committee, provides a forum for the discussion of policy issues, and is responsible for setting national-level Information Assurance policies, directives, instructions, operational procedures, guidance, and advisories for U.S. Government (USG) departments and agencies for the security of National Security Systems through the CNSS Issuance System. The CNSS is directed to assure the security of NSS against technical exploitation by providing: reliable and continuing assessments of threats and vulnerabilities and implementation of effective countermeasures; a technical base within the USG to achieve this security; and support from the private sector to enhance that technical base assuring that information systems security products are available to secure NSS.

The increasing threats inherent in ever changing and complex cyberspace makes the need for increased and continuing synergy within the CNSS Membership and between industry, academia, and our foreign partners a crucial part of IA guidance formulation. Included in this combined effort is cybersecurity collaboration which the CNSS promotes among owners of Federal NSS, Federal non-NSS, and non-Federal systems. CNSS is the cornerstone for IA guidance collaboration efforts.

The Department of Defense chairs the committee. Membership consists of representatives from 21 U.S. Government Departments and Agencies with voting privileges, to include the Central Intelligence Agency, DIA, DoD, Department of Justice, Federal Bureau of Investigation, NSA, National Security Council, and all United States Military Departments. Members not on the voting committee include DISA, NGA, NIST, and the National Reconnaissance Office. The DoD CIO is one of the tri-chairs of this committee.

5. Position, Navigation and Timing Executive Steering Group (ESG)

The ESG consists of senior officials representing each member of the National Executive Committee. It also includes representatives from key agencies within various departments, such as the Air Force and the Federal Aviation Administration. The ESG is co-chaired by the Under Secretary of Transportation for Policy and the DoD CIO.

The ESG meets more frequently than the National Executive Committee. It provides a mechanism for elevating interagency issues to a senior level between National Executive Committee meetings. The ESG seeks to resolve issues that do not rise to the level of the Deputy Secretaries on the National Executive Committee. The ESG sets the agenda for the National Executive Committee meetings and makes recommendations on those issues that are presented to the Deputy Secretaries.

6. The National Telecommunications and Information Administration's Policy and Plans Steering Group (PPSG)

Established by the NTIA, the PPSG is an advisory group of senior political-level Federal officials advising the NTIA Administrator on spectrum policy and strategic plans. The group serves as a forum for issue resolution and harmonization as determined by the NTIA Administrator. The PPSG is currently advising the Assistant Secretary (in his/her capacity as NTIA Administrator) on spectrum reallocation matters as it relates to the President's 500 MHz broadband initiative, especially potential reallocation of spectrum bands currently being used by Federal agencies (including DoD) for commercial broadband.

The DoD CIO is a voting member, but not a chair or co-chair.

Improving Services to Customers

Required OMB content:

Describe how DoD regularly evaluates existing and planned customer-facing services in order to:

- *Measure customer use and satisfaction through analytics and other approaches (BXXA)*
- *Improve usability, availability, and accessibility of services, including optimization of services for mobile use (BXXB)*
- *Advance DoD performance goals (BXXC)*

The Digital Government Strategy (DGS) states that the IRM Strategic Plan, under the Improving Services to Customers section should:
Milestone 6.3:

- *Describe the overall DoD approach to utilizing the guidelines to improve digital services.*
- *Also describe use of performance measurement tools to make data-driven decisions on improving digital services.*
- *Include the incorporation of governance changes and other activities such as mobile optimization, customer feedback, and analytics.*

Milestone 7.2

- *Publish a plan for optimizing existing priority customer-facing services for mobile use and improving existing services.*

(BXXA and addresses first two bullets under DGS Milestone 6.3.) 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 IT services. Driven by measurements of customer use and both formal and informal assessments of customer satisfaction, continuous improvement of customer service across the DoD is supported by a set of policies and specific activities that include ensuring the accessibility of information and IT 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.

For DoD's public websites, the Department measures customer satisfaction using formal surveys (Foresee) and direct feedback such as comment forms, one-on-one meetings and telephone calls (i.e., if the customer is not satisfied, they initiate communication to tell DoD, which, while not a formally tracked measure, is effective in identifying areas for DoD to improve as resources are available).

With regard to measuring customer use of public websites, DoD participates in the Federal Digital Analytics Program (DAP), which GSA established to facilitate implementation of Digital Government Strategy's Milestone 8.2 (Implement performance and customer satisfaction measuring tools on all .gov websites). GSA's DAP provides Google Analytics (GA) as a free,

turn-key, shared capability to Federal agencies which enables DoD to have an instantaneous, agency-wide view of Web metrics.

The DAP reports 10 minimum common baseline performance metrics:

1. Visits
2. Total Page Views
3. Unique Visitors
4. Page Views per Visit
5. Average Visit Duration
6. Time on Page
7. Bounce Rate
8. New vs. Returned Visitor
9. Visits per Visitor for a Given Time Frame
10. Total Number of On-Site Search Queries

Implementation requires each Federal agency to simply add the GA code on public .gov websites. Although the GA code is only required on public .gov websites, some DoD organizations have expressed interest in using it on public .mil websites. GSA's DAP manager confirmed that agencies may use the GA code on public .mil websites as well and there is a growing implementation on those sites also. As of January 2015, DoD has implemented the GA code on 48 of 55 public .gov websites.

Additionally, DoDI 8550.01 "DoD Internet Services and Internet-Based Capabilities" will be updated to reflect the requirement for DoD Components to implement GA or other performance measuring tools on public .gov websites and will include the option to implement on public .mil websites.

DoD follows these Operational Tenets/Guiding Principles for improving customer services:

- The DoD sponsor of a service (e.g., DISA, NSA, etc.) accepts accountability for the end-user experience of that service, even where the sponsor does not control the entire service pathway. Accordingly, the sponsor will coordinate with the owners of each service pathway to identify and resolve issues as they arise.
- Proactive IT service management is paramount, which includes regular assessments of customer satisfaction.
- For each service, there is one set of performance outcomes that all providers in the supply chain are equally accountable for delivering against.
- Service descriptions and Service-level targets for user-facing services are defined in user and mission execution effectiveness terms, describing what outcomes users should expect from the use of the service.
- Service descriptions and Service-level targets for IT services other than user-facing services (e.g., resource-facing services, infrastructure services, or platform services) are defined in technical terms to support other IT services.

- Service Level Agreements (SLAs) are established that are centered on end-user experience performance expectations.
- Supply chain partnership relationships and responsibilities are explicitly understood between all parties, including intra-Agency relationships, formalized in MOUs, MOAs, SLAs, and Operation Level Agreements.
- Operational costs must be traceable to individual services.
- Self Service is key to reducing operational costs.

(BXXB) The DoD CIO has directed several actions to improve the usability, availability, and accessibility of services, including optimization for mobility use. These actions are intended to drive the Military Departments and DISA to plan and program for the modification of existing DoD enterprise applications for use on commercial mobile device platforms, and to establish the criteria, selection, and implementation of DoD enterprise applications for mobile deployment. Where practical, DoD enterprise applications will be available for use on mobile platforms. Organizations are also expected to plan and program for the origination of new DoD enterprise applications with the capability to operate on commercial mobile device platforms.

In accordance with the DoD Commercial Mobile Device (CMD) Implementation Plan, DISA currently offers version 1.0 enterprise-level MDM and Mobile Application Store (MAS) capabilities with a consolidated library to support the delivery of mobile services over commercial devices. A common DoD enterprise mobile application development framework is being established to enable interoperability across commercial mobile device platforms that leverage commercial capabilities, drive the use of standards, ensure compliance and security, and facilitate consistency among core functions. To promote efficiency and cost savings, DoD will establish procedures (including security accreditation reciprocity) to ensure that applications are available across the DoD enterprise to all users with similar requirements. The implementation of mobile and wireless security architectures—in accordance with DISA and NSA guidelines and standards—will enable the DoD enterprise level network infrastructure to support Sensitive But Unclassified (SBU) and classified mobile services. Implementation of mobile and wireless security architectures and integration with authoritative data sources will incorporate usability, availability, and accessibility of IT services across the DoD enterprise.

A DoD Component-level MDM service is an installed, supported, and managed MDM and/or MAS system that supports the DoD Component's mobile users. Lessons learned from Component implementations inform development, operation, and management of credential management, common infrastructure, and mobile application development. Components gather requirements, identify mobility pilot projects, and participate in specific pilots to guide DoD program decisions. Component mobility pilots and initial operational uses have been and will continue to be evaluated to determine the impacts of proposed technologies to DoD mobility

services. Systems engineering trade studies, architecture development, and cost/benefit analyses shall be made available to help guide acquisition decisions across the DoD community.

DoD CIO published a memorandum, "Department of Defense Commercial Mobile Device Pilot Consolidation," March 21, 2013, to evaluate current mobile device pilots to determine if pilot oversight and/or activities should be consolidated. Components were directed to register their pilot activities by May 15, 2013. Unless proper coordination with the DoD CIO was achieved, CMD pilot implementations were directed to cease activities by October 15, 2013.

DoD CIO published a memorandum, "Department of Defense Commercial Mobile Device Implementation Plan Update," November 22, 2013, to announce Initial Operating Capability for the DoD Commercial Mobile Enterprise. The first phase of the transfer to enterprise capability was the migration of DISA's mobility pilots. DISA's mobility pilots transferred to operational status by December 31, 2013. C/S/As are encouraged to work with the DISA Mobility Program Management Office (PMO) to integrate ongoing mobile programs with the DoD Commercial Mobile Enterprise capability.

Additionally, DoD's applicable policies and guidance are being evaluated and updated to reflect OMB's emerging guidance for improving usability, availability and accessibility of IT services, including optimization of IT services for mobile use. For example, requirements for responsive design for websites and Web Application Programming Interfaces (APIs) for web-based data services will be included in updates to DoDI 8550.01. DoD CIO is coordinating with the DCMO on publishing a memorandum on responsive design, which is currently in staffing.

(BXXC) Insofar as DoD has some customers that are internal to the Department, or external customers that are mission partners, DoD is developing and improving services that advance DoD's performance goals. For example, the broadening of DoD enterprise email throughout the Department is enhancing information sharing across Components, through greater access to global contact information (among other aspects). DoD CIO published a memorandum, "Designation of Department of Defense Enterprise Email as an Enterprise Service for the Joint Information Environment," September 5, 2013. Defense Connect Online, as a second example, enables individuals and teams to collaborate easily from multiple locations and thereby increase the operational and budgetary efficiency of the larger team in achieving their mission.

Governance for Mobile Optimization (re: DGS Milestone 6.3)

Note: The cost aspects of Mobile Devices as identified in DGS Milestone 5.3 are discussed in the "Commodity IT and Shared Services" section below.

Under the auspices of the DoD CIO Executive Board, the DoD CIO is pursuing a phased approach to mobility solutions leading to improved unclassified and classified mobile capabilities. DoD CIO will make the final decision on DoD enterprise mobility solutions with input from Components to ensure that they meet mission requirements and achieve best value for

the Department. Under direction from the DoD CIO Executive Board, DoD Components will participate in the CMD Working Group (CMDWG). The CMDWG will review and approve standards, policies, and processes for the management of mobility solutions and mobile applications on an ad-hoc basis.

The DoD CIO via the CMDWG in coordination with partners:

- Has developed CMD application development requirements in accordance with the DoD CIO Memorandum, "DoD Commercial Mobile Device (CMD) Interim Policy," January 17, 2012, and from lessons learned as a result of pilots and consolidated DoD Components, Federal agencies, and NSA mobility implementations. DISA Chief Technology Officer is currently authoring a memorandum on mobile application development.

- Has established Certification and Accreditation (C&A) requirements for mobile applications and ensure reciprocity across DoD Components and Federal agencies. DoD CIO is coordinating with the OMB, CNSS, NSA, National Information Assurance Partnership (NIAP), NIST, and other Federal partners to establish minimum security baselines for the Federal government. The Digital Government Strategy published Milestone 9.1 minimum security baselines on May 23, 2013. The DoD CIO continues to coordinate with the Digital Government Strategy and ISIMC's MTTT on completing the baselines. NSA, NIAP, NIST and the DISA Field Security Office are working together to streamline security guidance and approval processes for mobile platforms.

- Is establishing the authority approval process for mobile applications. DoD CIO is currently staffing a draft memorandum, "Department of Defense Mobile Application Security Approval Process" to direct responsibilities and processes to streamline the mobile application approval process to a 30-day cycle, in line with the vision outlined in the DoD CMD Implementation Plan where mobile applications can be quickly developed, purchased, certified, and distributed to DoD users.

- Is developing DoD enterprise-wide, DoD Component-wide, and single-purchase licensing procedures for mobile applications. The DISA Mobility PMO is implementing procedures to leverage Apple's Volume Purchasing Program when purchasing and deploying enterprise mobile applications.

- Is defining appropriate data formats and uses of data for mobile applications (e.g., data aggregation, geo-location, machine readable policies, etc.). DoD CIO is coordinating with the DCMO on publishing a memorandum on responsive design for mobile platforms, which is currently in staffing.

DISA established the DoD Mobility PMO in 2013 to provide guidelines for secure classified and unclassified mobile communications capabilities to the DoD on a global basis. Provision of these capabilities will be accomplished through the implementation of a mobility solution, either at the

DoD or Component level, with enterprise level mobile communications services, which will provide a Department-wide foundation for interoperability, security, access to information, and reliable service to the DoD Components. DISA and its partners achieved version 1.0 of the unclassified mobility capability on January 31, 2014 with iOS support and Release 2.0 on May 9, 2014 with Android support. Defense Mobility Unclassified Capability (DMUC) users in DISA will begin the phased transition to initial release 1.0 capabilities including the MDM system, MAS, approved devices list, supported cellular access, DoD PKI support, transition of approved applications and enterprise services for mobility including DoD Enterprise Email (DEE), the DoD Global Address List, Tier 2/3 Service Desk Support and Defense Connect Online. The next major release adds gateway support on the unclassified side and also an office capability package to enable editing of Word documents and other Microsoft Office items.

Governance and Management Processes

Required OMB content:

Describe the governance process DoD uses to ensure that current law and policy are followed when planning, prioritizing, funding, executing, and decommissioning IT investments. If there are differences in the way the governance process is implemented across organizational units, describe those differences and why they exist. At a minimum, address:

- *Scope of the governance process, including Investment Review Board and other Portfolio Governance Boards (as appropriate) along with delegation of authority to bureaus or other organizational units (as appropriate); (CXXA)*
- *Which DoD stakeholders are engaged, including "C"-level leadership; (CXXB)*
- *The valuation methodology used to comparatively evaluate investments, including what criteria and areas are assessed; (CXXC)*
- *How DoD ensures investment decisions are mapped to agency goals and priorities; (CXXD)*
- *A high-level description of the process used to assess proposed investments and make decisions, including meeting frequency and how often the process is updated; (CXXE)*
- *How DoD coordinates between investment decisions, portfolio management, enterprise architecture, procurement, and software development methodologies (CXXF); and*
- *DoD's IT strategic sourcing plan, to include processes for addressing DoD enterprise licenses. (CXXG)*

(CXXA) The Defense Department's IT governance presents a unique challenge when compared with other Federal agencies' not only in terms of its magnitude— constituting approximately one-half of the Federal Government's overall IT budget—but in its scope and complexity. The Department's FY13 IT budget request of approximately $37 billion includes funding for desktop computers, tactical radios, identity management technology, human resource systems, commercial satellite communications, financial management systems, and much more. These investments support mission critical operations that must be delivered in both an office environment and at the tactical edge on the battlefield. The Department's IT environment is even more complex when one considers that these investments operate in over 6000 locations worldwide, and support the unique needs and missions of the three Military Departments and over 40 Defense Agencies and Field Activities within the Department.

The DoD is increasing visibility about its IT expenditures through improved budget transparency resulting from DoD's use of enterprise IT services such as enterprise email, various data services, and portal technologies

Financial Improvement Audit Readiness

DoD's Financial Improvement Audit Readiness initiative is improving, standardizing, and reengineering financial management processes to gain efficiency in financial management operations to produce better financial information—including financial information regarding IT expenditures—to support decision making.

that are being implemented across all DoD Components. Further improvements to the Department's three core processes (requirements, budgeting, and acquisition) that provide greater transparency in the procurement of IT infrastructure solutions, will help the DoD achieve even greater efficiency and effectiveness across the IT portfolio.

The Department's IT governance processes center on the DoD requirements, acquisition, and budgeting processes: the JCIDS, DAS, and the PPBE system. Additionally, the Department has a Defense Business System oversight process for managing the business portfolio of systems.

JCIDS

JCIDS is the systematic method established by the Chairman of the Joint Chiefs of Staff for identifying, assessing, and prioritizing gaps in joint warfighting capabilities and recommending potential solution approaches to resolve these gaps. Chairman of the Joint Chiefs of Staff (CJCS) Instruction 3170.01 and the JCIDS Manual describe the policies and procedures for the requirements process.

JCIDS plays a key role in identifying the capabilities required by the Warfighters to support the National Security Strategy, the National Defense Strategy, and the National Military Strategy. Successful delivery of those capabilities relies on the JCIDS process working in concert with other Joint and DoD decision processes. JCIDS procedures support the Chairman and Joint Requirements Oversight Council (JROC) in advising the Secretary of Defense on identifying gaps and assessing joint military capability needs. JCIDS is a joint-concepts-centric capabilities identification process to enable joint forces to meet future military challenges. The JCIDS process assesses existing and proposed capabilities in light of their contribution to future joint concepts. The JCIDS process was created to support the statutory requirements of the JROC to validate joint warfighting requirements. JCIDS is also a key informing process for the DAS and PPBE processes. The primary objective of the JCIDS process is to ensure that the capabilities required by the joint Warfighter to successfully execute the missions assigned to them are identified with their associated operational performance criteria. This is done through an open process that provides the JROC the information they need to make decisions and validate required capabilities needs. The requirements process supports the acquisition process by providing validated capability needs and associated performance criteria to be used as a basis for acquiring the right capabilities to support the full range of Defense operations. Additionally, JCIDS provides the PPBE process with affordability advice supported by the capabilities-based assessment, and identifies capability gaps and potential materiel and non-materiel solutions. While it considers the full range of doctrine, organization, training, materiel, leadership and education, personnel and facilities solutions, for acquisition, the focus of JCIDS is on the pursuit of "materiel" solutions.

JCIDS acknowledges the need to project and sustain joint forces and to conduct flexible, distributed, and highly-networked operations. JCIDS is consistent with DoD Directive (DoDD)

5000.01 direction for early and continuous collaboration throughout the Department of Defense. JCIDS implements a capabilities-based approach that leverages the expertise of government agencies, industry, and academia. JCIDS encourages collaboration between operators and materiel providers early in the process. JCIDS defines interoperable, joint capabilities that will best meet future needs. The broader DoD acquisition community through the DAS process must then deliver these technologically sound, sustainable, and affordable increments of militarily useful capability to the Warfighters.

For major defense acquisition programs or major automated information systems subject to OSD oversight, the products of the JCIDS process directly support the Defense Acquisition Board (DAB) in advising the Milestone Decision Authority for major milestone decisions.

DAS

The DAS is the management process by which the Department acquires weapon systems, automated information systems, and IT services. Although the system is based on centralized policies and principles, it allows for decentralized and streamlined execution of acquisition activities. This approach provides flexibility and encourages innovation, while maintaining strict emphasis on discipline and accountability.

(CXXB) The USD(AT&L) is the Defense Acquisition Executive (DAE) (in OMB terms, the Department's Chief Acquisition Officer). The USD(AT&L) reviews the most costly and complex programs, which are Major Defense Acquisition Programs (MDAPs) categorized as Acquisition Category 1D (ACAT 1D) and Major Automated Information System (MAIS) programs categorized as ACAT 1AM and serves as the Milestone Decision Authority (MDA) for those programs. The DAB (or IT Acquisition Board for MAIS programs), chaired by the USD(AT&L), provides advice on critical acquisition decisions. DAB members are senior officials from the Joint Staff, the Military Departments, and staff offices within OSD, to include the DoD CIO, Comptroller (i.e., the Chief Financial Officer in OMB terms), the Under Secretary of Defense for Personnel and Readiness (i.e., the Chief Human Capital Officer in OMB terms), and the DCMO. Although the Deputy Secretary of Defense is designated as the Department's Chief Operating Officer, Title 10, USC §133 designates the USD(AT&L) as the Department's acquisition authority and therefore grants him the authority to supervise all acquisition in the Department.

The DAE may delegate decision authority for an MDAP or a MAIS to the DoD Component Head, who may, and generally will, delegate decision authority to the Component Acquisition Executive. Such delegation makes an MDAP program an ACAT 1C program and a MAIS program an ACAT 1AC program.

The DAB is further supported by a subordinate group in OSD known as an Overarching Integrated Product Team (OIPT). Each OIPT facilitates communication and vets issues before the DAB meets. At Milestone Decision Reviews, the OIPT leader provides the DAB members

with an integrated assessment of program issues gathered through the Integrated Product Team process as well as various independent assessments.

DoDD 5000.01, The Defense Acquisition System, provides the policies and principles that govern defense acquisition. DoDI 5000.02, Operation of the Defense Acquisition System, establishes the management framework that implements these policies and principles. The Defense Acquisition Management System is an event-based process. Acquisition programs proceed through a series of milestone reviews and other decision points that may authorize entry into a significant new program phase. Details of the reviews, decision points, and program phases are provided in the instruction, as well as specific statutory and regulatory information requirements for each milestone and decision point.

One key principle of the Defense Acquisition System is the use of acquisition categories, where programs of increasing dollar value and management interest are subject to increasing levels of oversight. DoDI 5000.02 identifies the specific dollar values and other thresholds for these acquisition categories. The most expensive programs are the MDAPs and MAIS programs. MDAPs and MAIS programs have the most extensive statutory and regulatory reporting requirements. Some elements of the Defense Acquisition System only apply to weapon systems, some elements only apply to automated information systems, and some elements apply to both.

(CXXC) The Analysis of Alternatives (AoA) is an important element of the defense acquisition process. An AoA is an analytical comparison of the operational effectiveness, suitability, and life-cycle cost (or total ownership cost, if applicable) of alternatives that satisfy established capability needs. Initially, after the Materiel Development Decision, the AoA is initiated to examine potential materiel solutions with the goal of identifying the most promising option, thereby guiding the Materiel Solution Analysis phase. Subsequently, an update to the AoA is initiated at the start of the Technology Development Phase and is reviewed at Milestone B (which usually represents the first major funding commitment to the acquisition program). The update to the AoA is used to refine the proposed materiel solution, as well as reaffirm the rationale, in terms of cost-effectiveness, for initiation of the program into the formal systems acquisition process. For Major Defense Acquisition Programs at Milestone A, the MDA must certify in writing to the Congress that the Department has completed an AoA consistent with study guidance developed by the Director, CAPE, in addition to meeting other certification criteria (10 U.S.C. § 2366a). For Major Defense Acquisition Programs at Milestone B, the MDA must certify in writing to the Congress that the Department has completed an AoA with respect to the program in addition to meeting other certification criteria (10 U.S.C. 2366b). Pursuant to DoDI 5000.02, the AoA is updated as needed at Milestone C.

In practice, AoA issues vary somewhat between AoAs for weapon and other tactical systems and AoAs for major automated information systems. For additional information see Section 3 of the Defense Acquisition Guidebook, which provides discussion about AoAs for weapon systems and for major automated information systems.

One alternative that always should be considered, prior to actual development of a new system, is obtaining the needed capability through strategic sourcing options. Strategic Sourcing is covered in the Commodity and Shared Services section of this plan.

PPBE

The PPBE is the Department's strategic planning, program development, and resource determination process. The PPBE process is used to craft plans and programs that satisfy the demands of the National Security Strategy, within resource constraints.

The purpose of the PPBE process is to allocate resources within the Department. Program managers and their staffs need to be aware of the nature and timing of each of the events in the PPBE process, since they are called upon to provide critical information that would influence resourcing decisions.

In the PPBE process, the Secretary of Defense establishes policies, strategy, and prioritized goals for the Department, which are subsequently used to guide resource allocation decisions that balance the guidance with fiscal constraints. The PPBE process consists of four distinct but overlapping phases:

Planning. The planning phase of PPBE is a collaborative effort by the Office of the Secretary of Defense and the Joint Staff, in coordination with DoD components. It begins with a resource-informed articulation of national defense policies and military strategy known as the DPG. The DPG is used to lead the overall planning process.

Programming. The programming phase begins with the development of a Program Objective Memorandum (POM) by each DoD Component. This development seeks to construct a balanced set of programs that respond to the guidance and priorities of the DPG within fiscal constraints. When completed, the POM provides a fairly detailed and comprehensive description of the proposed programs, including a time-phased allocation of resources (forces, funding, and manpower) by program projected five years into the future. In addition, DoD Components may have the opportunity to describe important programs not fully funded (or not funded at all) in the POM, and assess the risks associated with the shortfalls. The senior leadership in OSD (including the DoD CIO), the Joint Staff, and Combatant Commands review each POM to help integrate the DoD Component POMs into an overall coherent defense program. In addition, the OSD staff (which includes the DoD CIO), the Joint Staff, and Combatant Commands can raise issues with any section of a POM and propose alternatives with adjustments to resources. Proposed programmatic changes are presented to the leadership for review, and decisions are documented in the Resource Management Decision (RMD) document. DoD Components use the RMD to update their POM data sets which are then incorporated into the Department's Budget and FYDP and submitted to OMB as part of the President's budget request.

Budgeting. The budgeting phase of PPBE occurs concurrently with the programming phase; each DoD Component submits its proposed Budget Estimate Submission (BES) simultaneously with its POM. The budget converts the programmatic view into the format of the congressional appropriation structure, along with associated budget justification documents. The budget is focused on one year, but with considerably more financial details than the POM. Upon submission, each budget estimate is reviewed by analysts from the office of the Under Secretary of Defense (Comptroller) and OMB. Their review ensures that programs are funded in accordance with current financial policies, and are properly and reasonably priced. Proposed budget changes are presented to leadership for review and decisions are documented in the RMD document. DoD Components use the RMD to update their BES data sets which are then incorporated into the Department's Budget and FYDP and submitted to OMB as part of the President's budget request.

Execution. The execution review occurs simultaneously with the program and budget reviews. The execution review provides feedback to the senior leadership concerning the effectiveness of current and prior resource allocations. Metrics are used to support the execution review to measure actual output versus planned performance for defense programs. To the extent that performance goals of an existing program are not being met, the execution review may lead to recommendations to adjust resources and/or restructure programs to achieve desired performance goals.

Defense Business System Governance

(CXXE) The 2005 NDAA established the Department's defense business system investment management framework to address Congressional concern that the Department has continued to invest billions of dollars in systems that were not integrated and failed to provide timely and reliable financial and business information for daily operations. In response to this legislation, the Department created the Defense Business Systems Management Committee (DBSMC) and five Investment Review Boards (IRBs)—the Human Resources Management IRB, the Real Property Infrastructure Lifecycle Management IRB, the Financial Management IRB, the Weapon Systems Lifecycle Management IRB, and the Materiel Supply and Support Management IRB.

Since that time, the IRBs and the DBSMC (both of which the DoD CIO participates in) have certified and approved hundreds of defense business system development/modernization investments worth billions of dollars. As the IRB / DBSMC governance process has matured, its ability to provide oversight has significantly advanced. It has improved the collection of data by which it makes decisions along with improvements to its cross-functional approach to portfolio management and use of performance management. It has also adapted to additional legislative requirements, such as Section 1072 of the NDAA for FY 2010, which required the IRBs to conduct reviews of investments' Business Process Reengineering efforts.

Congress made additional changes to the IRB structure through Section 901 of the NDAA for FY 2012. These changes include consolidating the five IRBs into a single IRB chaired by the Department's Deputy Chief Management Officer and expanding the scope of the IRBs to look at all of DoD's business systems, including those in sustainment, rather than just new or modernizing systems. These changes are an important step forward in helping the Department to accelerate the transition away from the legacy environment into DoD's target business systems environment.

The Department has identified 15 essential end-to-end processes, such as Hire-to-Retire (in the human resource management functional area) and Procure-to-Pay (in the supply chain management area) that the DBSMC and the IRB are using to help make targeted investments in business IT capabilities and ensure those investments are interoperable, efficient and non-duplicative. These end-to-end processes, which are represented in the Department's Strategic Management Plan and the Business Enterprise Architecture, are being used to identify the sub-processes, systems, data standards, performance measures and laws, regulations, and policies necessary to improve DoD business and drive better IT implementations. This more holistic understanding of our business will allow the Department to make more informed DoD Enterprise-wide decisions.

The Department has made progress in this area by focusing on process improvement first, and then ensuring the right tools and governance structures are in place. The Business Enterprise Architecture is maturing and serves as a tool that guides DoD investment decisions as well as aligning the Department to common standards and approaches. The investment management process, from IRBs to the DBSMC, provides the Department with the ability to ensure planned investments fit the target environment, align to the architecture, and have successfully undertaken business process reengineering. These efforts, coupled with on-going work to reform acquisition of information capabilities, are delivering better results for the business operations that Warfighters depend upon.

DoD CIO Role in the Department's Governance and Management Processes

DoD's current IT governance approach is characterized by multiple, often overlapping senior governance committees, functional oversight committees and processes, advisory boards, and corporate boards, which have proliferated over time, resulting in many inefficiencies and sub-optimal decision-making.

Proposed Simplified IT Governance Structure

(CXXD and CXXF) Consistent with guidance in the Secretary of Defense's 4 December 2013 memorandum, "Information Guidance from the 2013 Office of the Secretary of Defense Organization Review," the DoD CIO will use the CIO Executive Board (CIO EXBD) and its subordinate governance structures to establish and implement a new single IT Governance process that incorporates all aspect of the DoD CIO assigned functions. The new governance

process also complies with guidance from the Deputy Secretary of Defense's 12 February 2012 memorandum, "Department of Defense (DoD) Chief information Officer CIO Executive Board Charter," to refocus and strengthen CIO EXBD.

The subordinate structure better serves the mission and goals of the DoD CIO community today. It streamlines the decision processes, reduces unnecessary duplication or overlap, combines related areas of governance, and eliminates obsolete or inactive IT advisory groups. It strengthens DoD CIO governance by leading innovation, specifying coordination lines, and aligning subordinate management bodies along a continuum that tracks to program life cycles. The governance process informs the DoD CIO's decision-making and recommendations to the Deputy's Management Advisory Group and the Department's decision processes (requirements, acquisition, and resourcing) to more rapidly deliver and sustain IT, IM, cyber, warfighter, business, intelligence, and information enterprise solutions for the Department.

The subordinate governance structure and processes are effective immediately and support the CIO Executive Board as an action-oriented forum to identify innovative solutions and investments that address enterprise-wide capabilities, to include such efforts as the JIE.

The DoD CIO governance structure and process provides the DoD CIO the means to:

- Identify innovative technologies and standards; define and review enterprise architectures and IT solutions in terms of business/warfighter data and applications, common security, innovations, technology standards, and enterprise procurements for software licenses, hardware, and services; through the Enterprise Architecture and Services Board.
- Articulate and synchronize C4 and cybersecurity strategies, threats and mitigations of vulnerabilities, operational cybersecurity awareness, compliance, corrective actions, connection authorizations and waiver authorizations through the C4/Cyber Leadership Board.
- Manage IT/IM/Cyber investments as portfolios; leverage existing mission area investment review processes; emphasize review of Information enterprise mission area investments; assess recommended solutions against business/warfighter/intelligence needs; prioritize development, modernization and enhancement of new capabilities; and sustain steady-state investments through the subordinate Cyber-Information Technology IRB.

These new boards consolidate and subsume JIE governance functions. Until the new IT governance structure is fully activated, the JIE Executive Committee will continue in its role of developing the JIE implementation direction, goals, and objectives, and providing implementation oversight and accountability. Activities of the JIE Planning and Coordination Cell and JIE Technical Synchronization Office will continue as currently defined in the JIE Management Construct dated 9 November 2012. The JIE Management Office will continue as the DoD CIO's office for overall management of JIE implementation.

(CXXG) DoD's efforts regarding the use of Strategic Sourcing - to include use of enterprise licenses - are described in the Commodity IT and Shared Services section of this document under the heading "Shared Acquisition Vehicles".

CIO Authorities

Required OMB content:
Describe how DoD policies, procedures and authorities implement CIO authorities, consistent with OMB Memorandum 11-29, "Chief Information Officer Authorities" (DXXA)

(DXXA) The DoD CIO supports OMB's view that the CIO should possess authorities, responsibilities and duties to ensure operating efficiency and effective programs and to be a financial steward with public funds. The DoD CIO has reviewed the desired list of CIO's outcomes as defined in OMB's Memorandum M-11-29, and given the Department's federated management model, found that no fundamental gaps in authorities were revealed.

The DoD CIO is positioned with appropriate responsibilities and authorities to improve operating efficiency, encompass portfolio and program management and focus on delivering IT solutions that support the mission and business activities in a secure and efficient manner. The Department's federated management model integrates and balances the CIO authorities outlined in M-11-29 with the additional specific CIO authorities contained with Title 10, Title 40, and Title 44 in a manner that achieves the desired outcomes of operational efficiencies.

The CIO Authorities Appendix to this plan provides a detailed response to each one of the 5 questions that OMB raised in their Passback document, along with some selected supporting documentation. The fundamental CIO statutory mandates are outlined in Table 4 below:

Table 4: CIO Statutory Mandates

Authoritative Source	Mandates
Title 10 U.S.C 2222	• The Secretary of Defense shall delegate responsibility and accountability for the defense business enterprise architecture content, including unambiguous definitions of functional processes, business rules, and standards, as follows: o The Chief Information Officer of the Department of Defense shall be responsible and accountable for the content of those portions of the defense business enterprise architecture that support information technology infrastructure or information assurance activities of the Department of Defense. • For purposes of subsection (g), the appropriate senior official of the Department of Defense for the functions and activities supported by a covered defense business system is as follows: o The Chief Information Officer of the Department of Defense, in the case of any defense business system the primary purpose of which is to support information technology infrastructure or information assurance activities of the Department of Defense.
Clinger-Cohen Act of 1996 (Title 40 U.S.C.)	• Establishes statutory position of agency CIO • Responsibilities include:

Authoritative Source	Mandates
	○ IT architecture ○ Promote efficient design & operation of major IRM processes, including improvement to agency work processes (business process reengineering) ○ Evaluate the performance of IT investments and advise agency head whether to continue, modify or terminate • Develop, maintain, and facilitate the implementation of a sound, secure, and integrated IT architecture
Federal Information Security Management Act (FISMA) (Title 44 U.S.C.)	• CIO responsible to ensure agency compliance including: ○ Designate Senior Agency Information Security Officer ○ Develop and maintain Agency-wide Information Security Program ○ Develop and maintain information security policies, procedures, and control techniques ○ Training and overseeing personnel with significant information security responsibilities ○ Assist senior officials concerning their information security responsibilities ○ Provide information security protections commensurate with the risk
OMB Circular A-130	• The Secretary appoints a Chief Information Officer, as required by 44 U.S.C. 3506(a), who must report directly to the agency head to carry out the responsibilities of the agencies listed in the Paperwork Reduction Act (44 U.S.C. 3506), the Clinger Cohen Act (40 U.S.C. 1425(b) & (c)), as well as Executive Order 13011. Military departments and the Office of the Secretary of Defense may each appoint one official. The Chief Information Officer must, among other things: (a) Be an active participant during all agency strategic management activities, including the development, implementation, and maintenance of agency strategic and operational plans; (b) Advise the agency head on information resource implications of strategic planning decisions; (c) Advise the agency head on the design, development, and implementation of information resources. (i) Monitor and evaluate the performance of information resource investments through a capital planning and investment control process, and advise the agency head on whether to continue, modify, or terminate a program or project; (ii) Advise the agency head on budgetary implications of information resource decisions; and (d) Be an active participant throughout the annual agency budget process in establishing investment priorities for agency information resources; • The Chief Information Officer monitors agency compliance with the policies, procedures, and guidance in Circular A-130. Acting as an ombudsman, the Chief Information Officer must consider alleged instances of agency failure to comply with the Circular, and recommend or take appropriate corrective action. The Chief Information Officer will report instances of alleged failure and their resolution annually to the Director of OMB, by February 1st of each year.

Authoritative Source	Mandates
OMB M-11-29 Chief Information Officer Authorities	1. Governance. CIOs must drive the investment review process for IT investments and have responsibility over the entire IT portfolio for an Agency. 2. Commodity IT. Agency CIOs must focus on eliminating duplication and rationalize their agency's IT investments. 3. Program Management. Agency CIOs shall improve the overall management of large Federal IT projects by identifying, recruiting, and hiring top IT program management talent. 4. Information Security. CIOs, or senior agency officials reporting to the CIO, shall have the authority and primary responsibility to implement an agency-wide information security program and to provide information security for both the information collected and maintained by the agency, or on behalf of the agency, and for the information systems that support the operations, assets, and mission of the agency.
OMB M-09-02 Information Technology Management Structure and Governance Framework	1. The Agency CIO has ultimate responsibility for the governance, management and delivery of IT mission and business programs within the Department, and has an effective operative means of meeting this responsibility. 2. The CIO has the authority to set Agency-wide IT policy, including all areas of IT governance such as enterprise architecture and standards, IT capital planning and investment management, IT asset management, IT budgeting and acquisition, IT performance management, risk management, IT workforce management, IT security and operations, and information security. 3. The Agency CIO shall be the lead agency official a) Responsible for ensuring all Agency business and mission policies, processes, and IT and IT-related programs comply with the Federal Enterprise Architecture; b) Ensures the organization's enterprise architecture data is visible c) Ensures IT and IT-related systems, assets and IT services do not unnecessarily duplicate those available from other Federal agencies, and are planned for and managed throughout their lifecycle; d) Included in budget execution, formulation, preparation, prioritization and presentation activities, including determining and evaluating IT resource requirements and initiating procurements or advancing to subsequent phases of system development and/or acquisition; e) Reviews the status and progress of projects and activities in the Agency IT investment portfolio to determine whether to continue, suspend, re-baseline or cancel projects or components thereof, including any associated current or planned acquisitions; and f) Has established means for ensuring investment management, risk management, information security, and systems development lifecycle management policy compliance

Authorities with Respect to Workforce Management

The DoD Chief Information Officer has cyberspace workforce management responsibilities identified in the Clinger-Cohen Act (1996) and the Paperwork Reduction Act (1995) (codified in 40 USC 11315 and 44 USC 3501 et seq, respectively) regarding hiring, training, professional development and overall IT human capital management. This authority was reiterated in OMB Memorandum M-09-02, "Information Technology Management Structure and Governance Framework," dated October 21, 2008. Additionally, the CIO has skill-specific training responsibilities regarding information security personnel identified in the Federal Information Security Management Act (44 USC 3544), and IT program management training responsibilities identified in OMB Memorandum M-11-29, "Chief Information Officer Responsibilities," dated August 8, 2011.

Consistent with these laws, DoD Directive 5144.02 gives the DoD CIO authority to provide guidance and oversight with regard to the recruiting, retention, training, and professional development of the DoD cyberspace workforce. Accordingly, the DoD CIO will assess the requirements for Department personnel regarding IRM knowledge and skill and conduct formal training programs to educate DoD program and management officials about IRM.

Cybersecurity Management

Required OMB content:

- *Summarize DoD's strategy for ensuring that IT investment and portfolio decisions align with the Administration's Cybersecurity Priority Capabilities and DoD's IT security goals and how DoD will continue to strengthen this alignment (EXXA)*

- *Describe DoD's approach to ensure all mission critical applications have the proper continuity of operation and disaster recovery capabilities such that DoD can support the proper level of continuity of Government operations in accordance with Federal statute and guidance. (EXXB)*

Goal 6: *Strengthen Cybersecurity,* which is included in the goals section of this plan, is aligned with the DoD CIO's FY13 Campaign Plan Area of Execution 6 and has evolved based on the Deputy CIO for Cybersecurity's Cybersecurity 2020 efforts. A primary area of focus for Goal 6 is defense of DoD's networks, systems, and data.

(EXXA) In July 2011, DoD published the DoD Strategy for Operating in Cyberspace (DSOC), stemming from strategic threads outlined in the 2010 Quadrennial Defense Review and 2010 National Security Strategy. Strategic Initiative 2 of the DSOC (Employ New Defense Operating Concepts to Protect DoD Networks and Systems) called for the implementation of constantly evolving defense operating concepts to achieve DoD's cyberspace mission. The Defense of DoD Networks, Systems, and Data Strategy responds to that requirement and identifies strategic imperatives to assure the protection and integrity of DoD cyberspace assets. This strategy spans DoD engagement with commercial and coalition partners, as well as DoD operations on unclassified and classified networks and is the cornerstone of DoD's IT security investments and portfolio decisions.

Key elements of DoD's strategy for ensuring its IT investments and portfolios support the Administration's priority cybersecurity capabilities, include:

- Strong authentication - identity authentication based on PKI and other cryptographic-based technologies is already building a foundation for protecting and sharing information within DoD as well as for collaboration with partners. There remains a lack of strong non-PKI methods for unambiguously authenticating users and linking them to their authorized activities which significantly limits DoD's ability to accurately identify adversaries who have gained unauthorized access. To address this, DoD is implementing enterprise authentication security architecture to mitigate cyberspace risk and vulnerabilities in DoD networks and information.

- Trusted Internet Connections (TIC) - DoD investments in reducing attack surfaces have improved the security posture of DoD networks, systems, and data. Prior to reduction in TIC

(within DoD, referred to as Internet Access Points (IAPs)), DoD maintained over 40 connections. With this reduction effort now completed, DoD has 10 IAPs. This reduction allows for improved, standardized cybersecurity measures, such as monitoring for intrusions, identity and authentication, and central collection of incident data.

- Continuous Monitoring - Cyberspace adversaries are becoming more skilled, sophisticated, and strategically minded, and dramatic advances in technology have exacerbated the challenge. In response, DoD is adopting new advances in automation and standards in continuous monitoring and risk scoring of asset, security, and configuration management. More dynamic monitoring—along with its associated goal of near real-time situational awareness—will be realized by improvements being made in the JIE's sensing infrastructure. Sensor deployment has begun at IAPs that will monitor network access and traffic flow in order to quickly assess risk to information security and implement risk management decisions.

(EXXB) DoDD 3020.26 Continuity of Government (COG) states that USD(P) shall serve as the DoD Continuity Coordinator per National Security Presidential Directive-51/Homeland Security Presidential Directive-20 and shall:

- Provide strategic guidance and policy direction for, and oversee, planning, programming, budgeting, and execution of DoD continuity programs.

- Develop and maintain a comprehensive continuity plan to support the Secretary and Deputy Secretary of Defense, and ensure that the focus of all DoD continuity planning, preparation, and execution is on ensuring ability to continue performing the DoD Mission Essential Functions (MEFs).

- Provide oversight with the DoD CIO, and in coordination with the Deputy Chief Management Officer (DCMO), of information systems and networks that are critical to the performance of DoD MEFs under all circumstances across the spectrum of threats.

- Develop, specify, and promulgate, in coordination with DoD CIO, CJCS, and DCMO, continuity requirements for the secure and integrated COG and Continuity of Operations (COOP) communications supporting National and departmental missions.

- Develop, in coordination with the CJCS, a comprehensive, multi-year continuity test and exercise program to evaluate and validate the readiness of DoD continuity capabilities, plans, procedures, facilities, communications, and execution.

DoD directly supports COG through the resilient and survivable capabilities of its National Military Command System that allows for a graceful degradation of operations across the threat spectrum up to and including nuclear warfare. DoD also has classified programs that provide COG support to the President, Vice President, national senior leadership (e.g., Category 1

Departments and Agencies), and to DoD leadership (e.g., Secretary, Chairman, and Combatant Commanders). These capabilities are not only resilient but also include data storage backup at diverse locations and redundant network operations across various command nodes. Further, as part of the acquisition process, all new programs of record requiring a certification and accreditation must address a comprehensive COOP strategy.

Additionally, DoD's JIE construct includes CDCs that will be connected by a secure, interoperable common architecture. CDCs and Enterprise Operations Centers will link the Joint Force Commander's Joint Cyber Center to vital cybersecurity reinforcement capabilities and information support resources to ensure mission critical applications have the proper continuity of operation and disaster recovery capabilities.

Cyberspace Workforce

Required OMB content:
Summarize DoD's approach to IT human capital planning, including the ability to build a future ready workforce to support the agency's strategic goals and objectives. (FXXA)

(FXXA) The DoD CIO exercises its workforce oversight responsibilities through various forums; the two primary avenues are the CIO Executive Board and the DoD civilian community management system. The DoD CIO is the designated IT Functional Community Manager (FCM) for the Department of Defense and works with Under Secretary of Defense for Personnel and Readiness (USD(P&R)) across a network of DoD Component IT FCMs to maintain the overall health of the DoD civilian IT workforce. Human capital planning efforts for the IT community are discussed within the biennially produced DoD Strategic Workforce Plan submitted to Congress. DoD military forces and the DoD civilian workforce, supported by a robust contractor community, comprise the total force cadre that supports the Department's goal to achieve strategic advantage within cyberspace through technological innovation, secure and resilient operating capabilities, agile IT acquisition, and fiscally sound resources management.

A very important element of the Department's out-year cybersecurity strategy is ensuring that the right workforce is in place. An initial response to the needs of the Department is the accelerated delivery of approximately 6,000 cyberspace operations personnel by 2015. The majority of this workforce will be comprised of IT and cybersecurity personnel performing network operations and Defensive Cyberspace Operations missions. These tranches are a manifestation of the importance of cyberspace in the national defense environment. The workforce must be properly sized, properly trained and have career paths that encourage growth and development of IT and cybersecurity related skills. The Department's IT modernization effort includes a strong Defensive Cyberspace Operations workforce component that is an integral part of the Department's larger cyberspace workforce.

The Department relies on a broad occupational spectrum of skilled personnel to support its warfighting and business needs. These include the military and civilian personnel who design, implement, and govern the JIE as well as operational personnel who can communicate and coordinate across DoD Component command structures to conduct cyberspace offensive, defensive, and sustainment missions. In order to maximize the effectiveness of this workforce, the DoD is in the initial stages of migrating its IT and cybersecurity workforces into a broader cyberspace workforce framework, which is aligned to the specialty areas established by the National Initiative for Cybersecurity Education.

In November 2013, the Department released the DoD Cyberspace Workforce Strategy. Strategy initiatives currently under development include the DoD Cyberspace Workforce Framework, which will provide a common understanding of, and lexicon for, consistently defining the DoD cyberspace population and the work they perform; a DoD policy issuance providing standardized

guidance for the management, qualification, and tracking of the cyberspace population; and baseline standardized training requirements for the DoD cyberspace workforce.

The Department has also established the Cyberspace Training Advisory Council to synchronize training and readiness standards for the various cyberspace skill sets. Additionally, DoD is evaluating and improving the offerings of several of its training activities and educational institutions. The Department currently partners with commercial cybersecurity certification providers on the development and improvement of cybersecurity certification testing. These partnerships will continue to evolve as the cyberspace workforce construct matures. The objective is to provide the DoD cyberspace workforce with an integrated learning continuum that provides a variety of training environments.

Managing Information as an Asset

Required OMB content:

Address requirements from the OMB IRM Strategic Plan tasking memo:

- *How DoD will promote interoperability and openness throughout the information life cycle and properly safeguard information that may require additional protection.*
  [Specifically address how information collection and creation efforts, information system design, and data management and release practices will support interoperability and openness (GXXA).]

- *Describe how DoD ensures that personal information, including personally identifiable information (PII) and CUI, is accessible only to authorized personnel and how frequently these controls are verified (GXXB).*

Additionally, the following agency requirements in the Federal Digital Government Strategy will be collected through the IRM Strategic Plan, Enterprise Roadmap and integrated data collection:

- *Section 1.2 -- Ensure all new IT systems follow the open data, content, and web API policy;*
- *Section 2.2 -- Make high-value data and content available through web APIs, apply metadata tagging and publish a plan to transition additional high-value systems;*

Information delivered by networks is the enabler of all DoD missions. It is paramount that all information is valid, timely, and accurate. Since 2000, the demand for information has grown exponentially, resulting in innovative methods for sharing data and greater reliance on networks. Increasingly, mission success depends upon the ability of our military commanders and civilian leaders to act quickly and effectively based on the most accurate and timely information available. Recognizing that information is a strategic asset, DoD leaders are striving to establish a robust, rapidly scalable, interoperable, and secure capability that allows all authorized users to access the information they need anytime, anywhere, and on approved devices of their choosing. The challenge is amplified because our adversaries try to use every opportunity to penetrate our critical infrastructure to capture, disrupt, or destroy our information and do harm to our forces.

There are several obstacles or factors that impede interoperability and openness in the Department of Defense today. One significant factor stems from much information residing in very tightly controlled network security enclaves, resulting in little visibility and lack of awareness by others of data that might be useful for their purposes. One reason such enclaves exist is a lack of trust by the data owner that potential consumers of the data have a legitimate purpose. A central aspect of DoD's approach to increase interoperability within the Department, therefore, relies on the implementation of a single security architecture (through the JIE) that better ensures the legitimacy of data consumers and reduces the number of such security

enclaves, thereby enabling far greater ability to discover and access existing data among authorized users across the Department.

(GXXA) The Department's implementation of the immediate and longer term milestones in the Federal Digital Government Strategy[7] will be completed and refined as a subset of the ongoing implementation of the JIE. The DoD CIO will continue to collaborate with the components of the Office of the Secretary of Defense and the major DoD Components to shift the Department's policies and guidance about the management of information[8] to an information-centric approach – a move from managing information as documents, to managing discrete pieces of open data and content[9] that will be tagged, shared, secured, and presented in ways that are most useful for the consumers of the information. IT Governance will be strengthened and streamlined to lead decisions and actions that will reduce waste and duplication, increase returns on IT investments, improve effectiveness of IT solutions, and increase interoperability through shared, DoD enterprise IT services, more web APIs, continued optimization of DoD information for mobile use (as practicable), and more mobile applications, all operating under a single security architecture.

Information Lifecycle

OMB Circular A-130 defines information management as "the planning, budgeting, manipulating, and controlling of information throughout its life cycle." The life cycle for information within the DoD information environment spans information creation, storage (both short-term and long-term Records Management), protection, dissemination, discoverability and accessibility, and use by applications and other computing services when and where needed. Within this environment, the integrity of information must be protected from unauthorized access, and if a breach occurs, the Department's information environment must respond in such a way that damage is minimized. The Department must similarly responsibly dispose of data that is not intended for long-term retention.

Promoting Interoperability and Openness/Safeguarding Information

Promoting openness of information in the Department is inextricably linked to safeguarding information, and those topics are therefore both addressed in this section. To ensure that all new IT systems follow the open data, content, and web API policy, as required by OMB's Digital Government Strategy, the DoD CIO is collaborating with other DoD Component heads/PSAs to

[7] "Digital Government Building a 21st Century Platform to Better Serve the American People" http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

[8] There are over 100 top-level DoD issuances (directives, instructions, and manuals) that specifically address data and information control, handling, marking, and processing and an even larger body of similar documents in the DoD Components.

[9] Open data and content is digital information that is structured and exposed in ways that makes it available for use beyond its system of origin, internal or external to the Department, platform independent, and machine readable.

analyze current policies and will make appropriate changes to directives and instructions as OMB guidance emerges and is finalized. These changes will enable high-value data sets that are appropriate for release to be made available through web APIs and where appropriate that metadata tagging will be applied. Whether it is appropriate to expose data from high-value systems through APIs is analyzed through the JCIDS and Business Capability Lifecycle processes, as well as the DoD data release process described below. In addition, the high-value datasets that are appropriate for release are being considered as possible candidates for publication on Data.gov in accordance with Deputy Secretary of Defense Memorandum, "Support for the Open Government Initiative," April 14,2010.

DoD's data strategy document DoDI 8320.02 (and related implementation instruction) establishes policies, assigns responsibilities, and prescribes procedures for securely sharing electronic data, information, and IT services and securely enabling the discovery of shared data throughout DoD. DoDI 8320.02 also promotes the shift from securing information mainly at the transport level to implementing the secure sharing of data, information, and IT services within the DoD IE and with mission partners. DoD has a number of initiatives aimed at managing access to assure the trustworthiness of data consumers outside the original, intended data community. These initiatives (including PKI and Host Based Security System (HBSS)) are covered in Cybersecurity Management. Ensuring confidentiality and integrity of information throughout its lifecycle is critical to maintaining end-user trust in DoD systems. The HBSS baseline is a flexible, COTS-based application to monitor, detect, and counter against known cyber-threats. The HBSS solution will be attached to each host (server, desktop, and laptop) in DoD and configured to address known exploit traffic using an Intrusion Prevention System and host firewall.

A central element of DoD's data strategy policy is to make information visible, accessible, understandable, trusted and interoperable throughout the lifecycle for all authorized users. However, some DoD data originates in proprietary solutions with unique data formats that inhibit interoperability, even if the data is exposed. To address these situations, the Department has a number of initiatives aimed at removing these obstacles. One initiative involves adoption of the NIEM, a standards-based approach to exchanging information. In order to comply with White House guidance on the adoption of reference information exchanges, DoD will adopt NIEM as the best suited option for standards-based data exchanges, rather than continue development of the DoD-developed C2 Core and Universal Core data exchange standards. This adoption will involve a series of phased implementations by Components/Programs using NIEM content, guidance, and tools in an integrated effort to transition current DoD data exchange standards, specifications, and policies to a NIEM-based approach. In addition, the DoD will work with the NIEM Program Management Office to create a Military Operations MilOps Domain as part of NIEM.

The NIEM efforts will improve interoperability within the Department, with other Federal, State, Local and Tribal Governments, as well as with other external mission partners. To facilitate the

transition to NIEM, the DoD CIO will lead the development of a DoD Data Framework to include targeted guidance on governance and technical direction regarding NIEM adoption. Specifically, the DoD Data Framework will build upon the existing DoD data strategy and will provide principles, rules and additional guidance for managing data artifacts to improve information sharing. This framework will provide a foundation for how DoD views, manages, and shares its data. Adoption of NIEM offers potential efficiencies, long-term development cost savings, streamlined governance, and most importantly, improved information sharing across the DoD and with our mission partners. Additional efforts to improve interoperability include tagging of data that is collected or created within DoD, and the use of the DoD Metadata Registry in the Data Services Environment to help expose that data.

Ensuring the interoperability of IT and NSS, a Title 10 DoD CIO responsibility, remains a high priority. In addition to previously discussed initiatives in IT standards and DoD enterprise IT services, the DoD CIO has established an interoperability certification process to ensure new and revised IT and NSS have clearly defined interoperability requirements prior to development, and that these requirements are fully tested and certified prior to network connection, in accordance with DoDI 8330.01. DoDI 8330 will expand the interoperability certification process to also validate interoperability within each DoD Component's IT portfolio, while increasing DoD-level visibility of these Component systems for potential joint application.

Data Releasability

In accordance with DoDI 5230.29, "Security and Policy Review of DoD Information for Public Release," official DoD information that is proposed for public release shall be submitted for review and clearance if the information meets specified criteria or discusses any of the critical topics listed in the instruction.

Information intended for placement on Web sites, or other publicly accessible computer servers, which are available to anyone, without access controls, requires review and clearance for public release if it meets the requirements of the procedures contained in the instruction. Review and clearance for public release is not required for information to be placed on either DoD Web sites or computer servers that restrict access to authorized users.

Freedom of Information Act

DoD 5400.7-R describes that DoD's policy is to conduct its activities in an open manner and provide the public with a maximum amount of accurate and timely information concerning its activities, consistent always with the legitimate public and private interests of the American people. A record requested by a member of the public who follows rules established by proper authority in the Department of Defense shall not be withheld in whole or in part unless the record is exempt from mandatory partial or total disclosure under the Freedom of Information Act (FOIA). As a matter of policy, DoD Components shall make discretionary disclosures of exempt

records or information whenever disclosure would not foreseeably harm an interest protected by a FOIA exemption, but this policy does not create any right enforceable in court.

In order that the public may have timely information concerning DoD activities, records requested through public information channels by news media representatives that would not be withheld if requested under the FOIA should be released upon request. Prompt responses to requests for information from news media representatives should be encouraged to eliminate the need for these requesters to invoke the provisions of the FOIA and thereby assist in providing timely information to the public. Similarly, requests from other members of the public for information that would not be withheld under the FOIA should continue to be honored through appropriate means without requiring the requester to invoke the FOIA.

Records Management

The Department's approach to records management focuses on four areas:

- Policy and Oversight: Update policies to reflect current business and technical environment while leveraging DoD enterprise efficiencies. For example, records management needs to account for records stored within cloud architectures.
- The Records Management community: Build a collaborative community and improve DoD-wide understanding of the contribution of Records Management to the mission.
- Systems development: Pursue Records Management solutions for the DoD enterprise and incorporate into DoD enterprise systems.
- The professional workforce: Develop a DoD Records Management workforce with the knowledge and support necessary to be effective.

The DoD CIO, as the designated Senior Agency Official, is leading the Department in responding to the NARA Directive issued in August 2012 that includes a number of goals, deliverables, and action items:

- Manage permanent electronic records in an electronic format
- Manage email in an accessible electronic format
- Identify 30-year old permanent records
- Certify Records Officers
- Provide DoD Records Management training
- Schedule existing paper and other non-electronic records
- Research automated technologies to provide automated management of digital record content
- Obtain external involvement in open source Records Management solutions (Federal CIO Council)
- Report to NARA on meeting Records Management requirements in cloud architectures
- Establish a Community of Interest to solve specific challenges

NARA currently approves Disposition Schedules on a DoD organization-by-organization basis: the Military Department's (MILDEPs), Joint Staff, OSD, Combatant Commands and other Components all have different schedules that are overseen by different appraisers in NARA. As a result, consistency has been a problem and the schedules are very detailed and reflect the former world of paper files. Moreover, NARA schedules do not incorporate current and emerging IT solutions, or more efficient search capabilities. The current system is overly complicated, disjointed and inefficient given the increasing volume of information that needs to be handled.

A Department working group with representation from each DoD Component's Records offices is working to create a common Disposition Schedule that significantly streamlines the current granular retention schedules by establishing larger aggregations, or "Big Buckets," within which to organize records.

Big Data

The Department is also working on efforts to further leverage the power of Big Data. For example, the Department is increasingly deploying UAVs and other sensor platforms that are collecting tremendous amounts of information at such rates as over a billion pixels per second. Without emerging big data capabilities, the Department would not have the ability to consume and make use of this valuable collection of information. Big data tools enable the Department to move from traditional decision support applications to predictive analysis and complex event processing, giving commanders greater insight into the battle space and its emerging threats.

So far, most of the Department's use of Big Data is happening within the Defense Intelligence Components, but interest in the capabilities is increasing within other areas. To this point, Defense organizations have been developing big data capabilities to meet their specific mission need and specific type of data. Moving forward, the Department needs a more strategic approach to establishing Big Data capabilities for the Defense enterprise. While individual organizations can benefit from their own implementations, greater benefit will be realized by establishing a fully integrated and synchronized Big Data infrastructure in DoD Non-Secure Internet Protocol Router Network and Secret Internet Protocol Router Network environments. The value that can come from big data analytics increases as more and more data can be accessed and analyzed within the particular big data environment. As the Department moves forward, big data capabilities will be established that support multiple types of missions and incorporate data from a wide range of sensors and collectors.

Ultimately, achieving the full potential of Big Data efforts depends upon high-volume data streams providing input. This objective will require the Department to improve the efficiency and effectiveness of its information infrastructure to backhaul data from all Big Data sources in support of analysis, prediction and production.

Privacy

(GXXB) The Defense Privacy and Civil Liberties Division (DPCLD) implements the Defense Privacy Program and establishes policies, provides workforce training, reviews and comments on Department issuances to ensure Department-wide compliance with the Privacy Act of 1974 and Privacy Program issuances (DoDD 5400.11, "DoD Privacy Program," and DoD 5400.11-R, "Department of Defense Privacy Program"). The Defense Privacy Program's policies require the Department to incorporate appropriate administrative, technical, and physical safeguards, based on the media (paper, electronic, etc.) involved and provide guidance regarding the access to personal information by individuals when such information is maintained in a Privacy Act system of records, and the privacy, confidentiality, and security requirements for personally identifiable information (PII) and controlled unclassified information to prevent compromise or misuse during storage, transfer, or use of PII. These policies include work performed at authorized alternative worksites.

The Department of Defense takes its responsibility seriously to safeguard PII in its possession and to prevent theft, loss or compromise of PII. As a principle, privacy is designed into DoD systems. The DoD CIO works with DPCLD 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). The DPCLD and CIO actively collaborate on FISMA quarterly and annual reporting which includes reviews of SORNs and PIAs compliance across DoD.

The DoD IT PIA program protects the privacy of individuals by systematically ensuring controls are in place to protect data, and by assessing and minimizing vulnerabilities of DoD information systems containing PII. The PIA Program:

- Establishes PIA policy, DoDI 5400.16 "DoD Privacy Impact Assessment Guidance," and procedures to reflect current and new 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 Components to assist with establishing and maintaining PIA programs that increase the completion rate of PIAs in compliance with the law.

Per OMB and DoD guidance, PIAs are required to be performed and updated as necessary where 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. In addition, every three years a PIA has to be reevaluated to ensure any changes to the system that could have privacy impact are reviewed and appropriately updated as part of the C&A process.

Commodity IT and Shared Services

Required OMB content:

Address detailed requirements from the OMB IRB Strategic Plan tasking memo, including DoD's:

- *Approach to maturing the IT portfolio, to include optimizing commodity IT (including data centers), rationalizing applications and adopting a service orientation approach (HXXA)*
- *Plan to re-invest savings resulting from consolidations of commodity IT resources (including data centers)(HXXB)*
- *Approach to maximizing use of inter- and intra-agency shared services (such as those enabled by common platforms and lines of business) and shared acquisition vehicles for commodity IT, such as those determined by the Strategic Sourcing Leadership Council, in order to reduce duplicative contract vehicles (HXXC).*

[From Digital Government Strategy memo dated 3/18]
Milestone 5.3: Agencies should describe their overall approach to drive down costs of mobile devices and services. This can include strategic sourcing activities or Agency-wide consolidation of mobile/wireless contracts as a result of the inventory created through milestone 5.2

(HXXA) The Defense Department's IT investments are critical in supporting our military forces in their mission of protecting our Nation's security. These investments support the effective and efficient use of information as a strategic asset in military and business operations to improve the operational effectiveness and security of the information and networks transporting the information.

The DoD has been engaged in data center consolidation for many years through individual DoD Component activities (e.g., NMCI) and broader Department efforts (e.g., DECC). In 2010, the FDCCI brought data center consolidation to the forefront as a principal lever to achieve enhanced capability delivery, improved cybersecurity, and efficiencies (savings). Currently, nearly 50% of all DoD data centers are planned to close within the FYDP with the remaining data centers transforming and conforming to JIE standards.

Detailed cloud computing implementation planning has been ongoing and informs the JIE projected plan of actions and milestones. The 10 Point DoD IT Modernization Plan defined three key objectives focused on: consolidating Enterprise networks (including network operations, servers, applications and data centers); developing the DoD Enterprise Cloud (EC); and standardizing IT platforms and processes that ensure a secure cyber environment.

The DoD Cloud Computing Strategy provided an initial approach to move the Department from the current state of a duplicative, cumbersome, and costly set of application silos to an end state of an agile, secure, and cost effective service environment that can rapidly respond to changing mission needs. Cloud computing will enable the Department to consolidate and share commodity

IT functions resulting in a more efficient use of resources. Cloud services will enhance Warfighter mobility through device and location independence while providing on-demand secure global access to mission data and enterprise services. Cloud platforms and services can provide increased opportunity for rapid application development and reuse of applications acquired by other organizations.

Done correctly, cloud computing represents a significant opportunity to improve the performance, efficiency and security of DoD IT. To achieve this vision, the DoD CIO continues to work with other senior leaders at the Pentagon to ensure that we are delivering the right policies and guidance to drive the appropriate adoption of cloud computing.

Additionally, the Department is emphasizing the increased use of commodity purchasing of hardware, software, and IT services as a major means of achieving efficiencies. Through the sharing of purchase agreements across organizations within the Department, DoD is able to minimize the number of purchase vehicles in use, further streamlining our IT acquisition processes.

To date, the Department has achieved cost avoidance estimated at over $3 billion over a 10 year period through the Enterprise Software Initiative (ESI). DoD organizations have achieved significant efficiencies in the purchase of software, hardware and IT services from the open market as a result of terms and conditions negotiated with vendors whose products appear in the ESI inventory.

(HXXB) In recent years, DoD's reinvestment of savings from IT efficiencies has not necessarily been re-directed back to IT programs or initiatives. These funds (from savings or cost avoidance) are generally redirected to the programs that are determined to provide the most improvement to Defense-wide Warfighting capability and readiness.[10]

For instance, on January 6, 2011, then Secretary of Defense Gates announced a series of decisions regarding Department efforts to realize at least $100 billion in savings that the Military Departments could keep and shift to higher priority programs. To achieve the savings targets, Service leadership conducted a thorough and vigorous scrub of bureaucratic structures, facilities, programs (including IT), business practices, civilian and military personnel levels, and associated overhead costs. The measures rebalanced the Department's spending habits while increasing investments in proven capabilities most relevant both to current wars and to the most likely future threats.

Under these measures, the Military Departments were informed they would keep the savings they found and reinvest in the capabilities each Service needs to support the Warfighter. The announcement stated that the bulk of the savings would be used by the Military Departments to

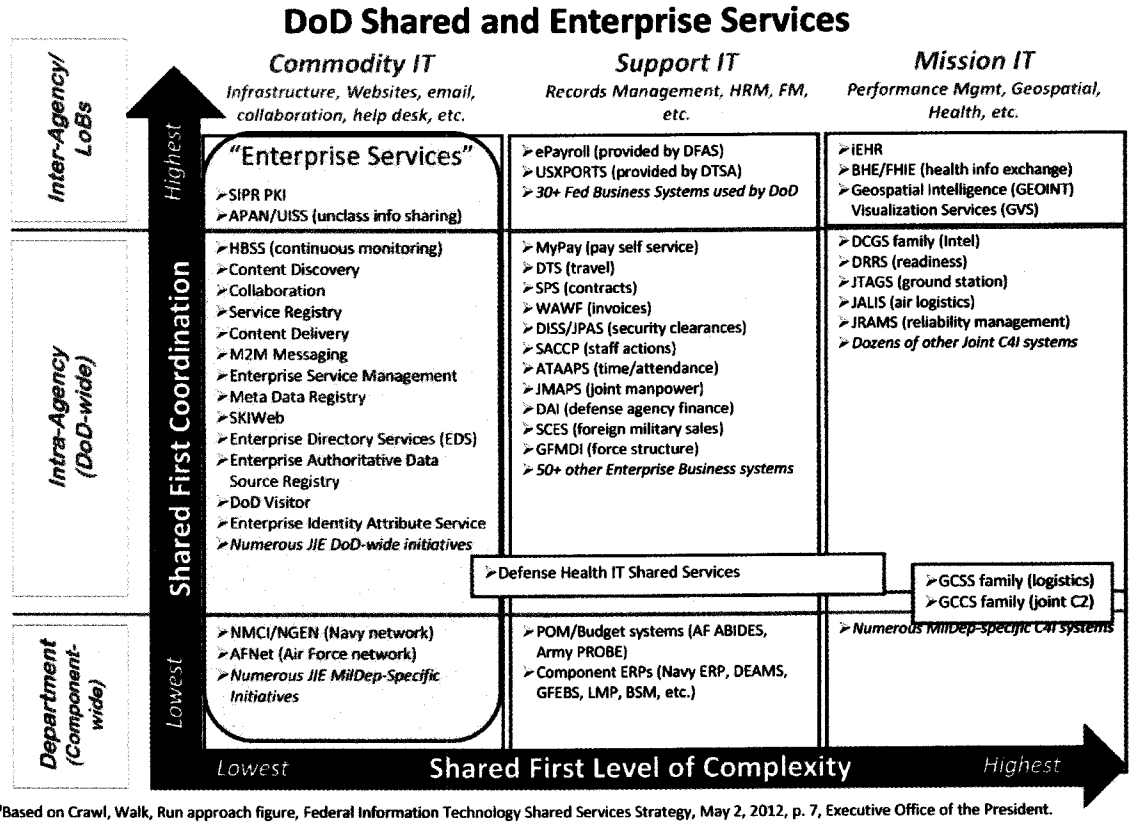
[10] Text in this and the next two paragraphs is based on the text of the press release at the following URL: http://www.defense.gov/Releases/Release.aspx?ReleaseID=14178

make key investments in areas such as ship building, long-range strike, missile defense, intelligence, reconnaissance and surveillance, wounded warrior care and facilities, and much more.

(HXXC) DoD continually faces the challenge of making best use of constrained funding to provide the required capabilities to support its mission. Shared Services are one method to drive down operating costs by providing economies of scale in buying power and reducing duplication of effort. Shared services are not new to the Department. The 17 Defense Agencies, 7 Field Activities, and US Transportation Command were established progressively over the last 60 years with each having a mission of providing a designated set of shared business services across DoD. DISA was established with the mission of providing shared IT infrastructure.

DoD's shared IT services efforts, informed by the OMB Shared Services Strategy, are categorized in three major groups: commodity IT, support, and mission, as shown in Figure 2 below.

Figure 2 - DoD Shared and Enterprise IT Services



[1]Based on Crawl, Walk, Run approach figure, Federal Information Technology Shared Services Strategy, May 2, 2012, p. 7, Executive Office of the President.

Note: Listing is as of 19 April 2013. Illustrative examples only. Not a complete listing.

As indicated by Figure 2, DoD has already implemented a significant number of mature shared IT services in all three categories.

The priority focus for DoD CIO going forward is on the group of Commodity IT Enterprise Services enabled by implementation of the JIE. While the DoD CIO is focused on this set of IT services, other parts of DoD continue work to implement other shared services. In particular, the Defense Business System certification requirements in 10 U.S.C. 2222 are accelerating adoption of a group of core systems in major functional areas, such as Financial Management, Human Resources, and Installations and Environment.

Where appropriate, DoD explores opportunities to implement shared services within or between a set of its Components, across the Department, and to other Federal Agencies. The Department and its Components currently have numerous shared services, including pay and time reporting systems, common access services, personnel systems, administrative and management, and many others. As discussed elsewhere in this document, the JIE is the overarching effort under which most Department-wide commodity IT shared services will be implemented.

As DoD examines the potential for additional shared services, it takes into consideration:

- Key objectives and ability to carry out Mission
- A business case to determine potential for cost savings, efficiencies, and resource maximization
- Scalability

Infrastructure shared IT Services are enabled by the efforts to move the Department to the JIE. The JIE will provide a secure joint information environment, comprised of shared IT infrastructure, DoD enterprise IT services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies.

Business-focused shared IT services are enabled by central organizations with standard processes. While there are some savings possible where shared IT services are provided independent of organizational alignment, the most efficient, effective examples of shared services savings to date have come from the consolidation of organizational function, personnel, and technology solutions to provide the full spectrum of shared capabilities. A success story in the Commodity IT Enterprise Services group is DEE.

CASE-IN-POINT: Defense Enterprise Email

The DEE service provides secure cloud-based email to the DoD enterprise that is designed to increase operational efficiency and facilitate collaboration across organizational boundaries. As an enterprise-wide service, DEE reduces the cost of operations and maintenance by consolidating hardware into DISA's secure, global DECCs. DEE creates a common platform for the DoD, ensuring Defense Components can easily and effectively share information among virtual groups that are geographically dispersed and organizationally diverse.

Shared Acquisition Vehicles

DoD is participating in the Strategic Sourcing Leadership Council (SSLC), which is working to identify new opportunities to pool the government's buying power and reduce the need for duplicative contracts. Since its inception, the SSLC has been conducting spend analyses of opportunities for strategic sourcing, analyzing spend management alternatives and their measures of success, and analyzing current sourcing strategies. The Council has formed 13 teams focused on commodities that have been identified as areas of opportunity:

1. Education and training services
2. Large enterprise software/relational database management systems
3. Information technology equipment
4. Conference space and planning
5. Medical and lab
6. Virtualization software
7. Fuel/lubricants
8. Janitorial/sanitation supplies
9. GSA SmartBUY program with Microsoft
10. Research and subscriptions (e.g., those used by Library of Congress)
11. Supplies used for maintenance, repair, and operations
12. Furniture
13. Rental cars

DoD is participating in 12 of these commodity teams, with the DLA leading one (Fuel/lubricants) on the Department's behalf. Commodity team members from DoD represent OSD, the Military Departments, DoD CIO, DLA, Defense Acquisition University, and Defense Travel Management Office.[11]

A pilot effort to capture the prices that agencies pay for commonly used goods and IT services will be established so that contracting officials, program managers, and those conducting market research can identify the best prices. This pilot is a key component of efforts to accelerate the pace of savings recommended by SSLC. SSLC will continue to work to identify new opportunities to pool the government's buying power and reduce the need for duplicative contracts.[12]

---

[11] SSLC Established to Lead Government Sourcing Efforts, News, Defense Procurement and Acquisition Policy Defense Pricing, January 25, 2013, http://www.acq.osd.mil/dpap/ss/news/index.html#jan18-13.

[12] Building a 21st Century Government by Cutting Duplication, Fragmentation, and Waste, Office of Management and Budget, The White House, April 9, 2013, http://www.whitehouse.gov/omb/Building_a_21st_Century_Government_by_Cutting_Duplication_Fragmentation_and_Waste.

One of DoD's primary thrusts with shared acquisition vehicles is the DoD ESI. DoD ESI has long-standing relationships with numerous COTS software publishers and their government resellers, and has also been building enterprise-level relationships with several commercial IT hardware vendors that provide proprietary software and IT services for their hardware products. Under DoD ESI, Enterprise Software Agreements (ESA) have been established for most of the COTS software products that are widely used across DoD. DISA and other DoD Components will use these ESA (where possible) to create Enterprise License Agreements (ELA) for widely used products to which all DoD Components will have access. In addition, the DoD Enterprise Solutions Steering Group will continue to identify near-term solutions for computer network defense and fund DoD-wide ELA for anti-virus, anti-spyware, firewalls, secure configuration compliance validation initiative tools, and the HBSS.

DoD is deploying several commodity IT hardware contract vehicles for items such as desktops, laptops, monitors, printers, and multi-function devices, which makes this hardware relatively simple and more cost-effective to acquire, once the buyers establish baseline performance and security specifications. For instance, the Army uses the Army Consolidated Buy process; the Air Force uses the US Air Force Quantum Electronic Buy process; and Navy commodity IT hardware needs are typically met through the NMCI/Next Generation Enterprise Network contracts. Marine Corps users are provided for through the Marine Corps Common Hardware Suite. DoD Component owners of these vehicles will include additional commodity IT hardware (e.g., mobile devices) and incorporate jointly developed buying standards into the target contracts. The remaining DoD Components procure commodity IT hardware through a wide variety of contract vehicles. DoD CIO, in coordination with MILDEPs and DISA, will guide and assist future DoD enterprise IT commodity acquisitions by: collecting and analyzing current and planned DoD Component spend; establishing joint buying standards for commodity IT hardware, engaging with key publishers and manufacturers on their technical roadmaps, and formulating policy and regulations favorable to the process.

To codify this approach, a policy memorandum will be co-signed by DoD CIO and AT&L, describing the COTS software approach mentioned above and mandating use of the DoD enterprise commodity IT hardware procurement vehicles. Appropriate language will be drafted to staff through the Defense Acquisition Regulations Council, for inclusion in the Defense Federal Acquisition Regulation Supplement.

Overall Approach to Drive Down Costs of Mobile Devices and Services (re: DGS Milestone 5.3)

The DoD's overall approach to mobile cost management includes several initiatives. Mobile solutions will be selected to meet mission requirements and achieve best value for the Department. Commercial devices and solutions and accreditable cloud solutions are being considered, to the greatest extent possible, to reduce costs and DoD ownership and management of infrastructure. A multi-vendor mobile operating system environment for CMDs is being supported to enable a device-agnostic procurement approach. Multiple form factors of CMDs are

being supported and encouraged in order to meet the various operational use case scenarios. A storage and distribution facility with federated management has been established for mobile applications. Mobile applications are being certified via an approved governance process. A common mobile application development framework is being established to enable interoperability across OSs. The framework shall leverage commercial capabilities, drive the use of standards, ensure compliance with security requirements, and facilitate consistency among core functions.

Mobile Device Management MDM services for control and audit of CMDs have been established and are being managed at the DoD enterprise level to optimize operation and maintenance, ensure security, and support CMD synchronization. DoD enterprise MDM services are improving upon the quality of service of Component MDM services. The DISA Mobility PMO achieved version 1.0 of the DoD Commercial Mobile Enterprise on January 31, 2014. DISA's DMUC and Defense Mobility Classified Capability (DMCC) incorporate many of the cost management controls.

The DoD CIO will conduct a semiannual audit that determines the total cost of mobility implementation, operation, and management. DoD CIO and USD(AT&L) published a memorandum, "Department of Defense Inventory of Mobile Devices and Wireless Contracts," March 15, 2013, to direct Components to conduct an inventory of their wireless service contract and mobile device information and report results to the DoD CIO by April 5, 2013. DoD CIO and USD(AT&L) used the inventory results to complete the Digital Government Strategy Milestone Action 5.2 on May 23, 2013.

Acquisition contracts for CMD carrier services (e.g., mobile voice and data via cellular) are being consolidated, to the greatest extent practical, and Department- and government-wide contracts are preferred to promote efficient use of government resources, in accordance with the Digital Government Strategy. DoD CIO and the DISA Mobility PMO have coordinated with the DoD Components and the GSA FSSI to identify and recommend three primary contract vehicles for commercial wireless services for the DoD community – the Next Generation Wireless Blanket Purchase Agreements (BPA) (Army, Air Force), Naval Supply Systems Command Fleet Logistics Center San Diego (Navy), and GSA Wireless FSSI BPA. In addition, Defense Information Technology Contracting Office has established a contract vehicle to address international roaming services.

CMD carrier service accounts and usage will be managed and monitored using a TEM system that regulates underutilized and over-subscribed accounts. Navy has established a TEM system, and other Components are investigating TEM services. The DISA Mobility PMO is establishing a DoD-wide TEMS service.

The CMDWG, previously introduced in the Improving Services to Customers section) has the following functions related to cost management:

- Develop CMD and MDM solution requirements in accordance with the DoD CIO Memorandum, "DoD CMD Interim Policy," dated January 17, 2012, and from lessons learned as a result of pilots and consolidated mobility implementations accomplished by DoD Components, Federal agencies, and NSA.
- Assess Business Case Analyses and recommend standards, policies, and processes for the development and management of mobility solutions.
- Assess semiannual audits for comparison of mobility service approaches and recommend metrics to aid decisions on optimal management of implementation options; examples may include:
    - Evaluate inventory annually and identify: Commercial Carrier, User, Plan(s), Device (Manufacturer, Model, Operating System, Electronic Serial Number per device)
    - Compute Average Cost Per Unit where unit is a CMD
    - Identify Cost Per Megabyte (MB) Equivalent (includes data, voice, text)
    - Identify MB Equivalent Usage and Growth
    - Identify savings and cost avoidance compared to prior year
    - Identify overage charges and appropriate action plan
    - Identify under-utilized or zero usage devices and appropriate action plan

Cognizant of the Secretary's Information Technology Efficiencies initiative, DoD CIO published the DoD CMD Implementation Plan on February 15, 2013. DoD will use an evolutionary acquisition approach to deliver unclassified and classified mobility capabilities to the DoD enterprise in a manner that significantly reduces cost, eliminates duplication, and promotes economies of scale. DoD CIO is executing the Implementation Plan to equip users and managers with mobile solutions that leverage commercial off-the-shelf products, improve functionality, decrease cost, and enable increased personal productivity. DISA's DMUC and DMCC incorporate many of the cost management controls.

The Digital Government Strategy relies heavily upon the GSA to establish and administer federal mobility services. It directs the GSA to establish a government-wide contract vehicle for mobile devices and wireless service; set up a government-wide mobile device management platform to support enhanced monitoring, management, security, and device synchronization; and establish a Digital Services Innovation Center to improve the government's delivery of digital services. The Implementation Plan enables DoD Components to contract for mobility services from GSA once the GSA-provided MDM/MAS support meets the appropriate DoD-level security requirements. Instantiated MDM/MAS systems must report and pass network management information to DoD-level network management systems per current USCYBERCOM requirements. DoD will continue to evaluate GSA-developed MDM/MAS solutions as they become available. In

addition, DoD CIO will participate in Digital Government Strategy initiatives and assist GSA with the development of mobility requirements for federal mobility services.

DoD enterprise mobility solutions will be established to ensure that they meet mission requirements and achieve best value for the Department. DoD CIO will, in coordination with the USD(AT&L), define the appropriate methods to measure the total lifecycle cost of mobility services. DoD submitted contributions to the Digital Government Strategy Milestone #5.2 inventory of CMDs and wireless service contracts. The DoD CIO will conduct a semiannual audit that determines the total cost of mobility implementation, operation, and management and will review and assess semiannual audits to determine optimal management of mobility service solutions. USD (AT&L) will assist the DoD CIO and the CMDWG in crafting approaches for the acquisition of services to support the goal of acquiring cost effective secure classified and protected unclassified mobile solutions for the Department.

Accessibility

Required OMB content:

Address the following OMB IRM Strategic Plan tasking memo requirements:

- *Creating a diverse environment where individuals of all abilities can work, interact, and develop into leaders (IXXA)*
- *Integrating accessibility considerations into the processes used in developing, procuring, maintaining, or using IT (IXXB)*
- *Building workforce skills to support an environment where Section 508 requirements and responsibilities are well understood, communicated, implemented, and enforced (IXXC)*

(IXXA) According to the 2010 Census, there are 56.7 million Americans with disabilities.[13] Among these are 125,000 Federal employees with a disability or functional limitation.[14] The DoD Civilian workforce alone includes 5,091 DoD employees with targeted disabilities.[15]

Section 508 was enacted to eliminate barriers in IT, to make available new opportunities for persons with disabilities, and to encourage development of technologies that will help achieve these goals. DoD is actively engaged in efforts, led by the Office of the Under Secretary of Defense for Personnel and Readiness, to:

1. Recruit qualified individuals with disabilities into the DoD workforce and recognize the outstanding contributions of DoD employees with disabilities through an annual DoD awards program, both in accordance in accordance with DoDD 1440.1, "The DoD Civilian Equal Employment Opportunity (EEO) Program," May 21, 1987.

2. Maintain records of the number of DoD employees with self-identified disabilities and of the accommodations provided to them in accordance with Section 504 of the Rehabilitation Act of 1973, as amended, as codified in Section 794 of Title 29, United States Code.

3. Work with the DoD Component Section 508 coordinators and Equal Employment Opportunity officials to resolve complaints of alleged DoD non-compliance with Section 508.

The Office of the DoD CIO, meanwhile:

1. Develops policies, procedures, and requirements related to achieving implementation of, compliance with, and institutionalization of Section 508.

2. Designates a DoD Section 508 Coordinator to serve as the DoD point of contact for Section 508 implementation.

---

[13] "Americans With Disabilities: 2010, Household Economic Studies," Current Population Reports by Matthew W. Brault, Issued July 2012, P70-131, U.S. Census Bureau.
[14] Executive Order 13548 of July 26, 2010, "Increasing Federal Employment of Individuals With Disabilities,"
[15] Defense Manpower Data Center, February 2014.

The Office of the DoD CIO also conducts reviews of DoD websites to ensure accessibility. The goal for public website evaluations is for each DoD Component to reach 100% compliance. Evaluation results are sent to Component Section 508 Coordinators, Section 508 POC, and Webmasters to help improve future evaluations.

The current Section 508 Standards, which were mandated by Section 508 and are presently in revision, are here: http://www.section508.gov/index.cfm?fuseAction=stdsdoc

In addition to any applicable technical standards, solicitations should also reference:

1194.31 Functional Performance Criteria

1194.41 Information, Documentation and Support

The GSA is statutorily charged with providing Federal Agencies with technical assistance in implementing Section 508. To that end, GSA conducts monthly random reviews of DoD solicitations posted to the FedBizOpps website. GSA alerts the Contracting Official involved, as well as the DoD and DoD Component Section 508 Coordinators, regarding those solicitations that are deemed non-Section 508-compliant. The Section 508 Coordinators then work with the Contracting Official, in coordination with the OUSD(AT&L), to resolve the compliance issue.

(IXXB) Section 508, as amended, requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they shall ensure that the electronic and information technology allows Federal employees with disabilities and members of the public with disabilities access to and use of information and data that is comparable to the access to and use of data by Federal employees and members of the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Undue burden is defined as significant difficulty or expense, per Subparts 39.2, 39.203(c)(2), and 10.001 of Subchapters B and F of Volume 1, Federal Acquisition Regulation, and a finding that undue burden exists does not absolve the Department of the requirement to provide comparable access to persons with disabilities.

On June 3, 2011, the DoD CIO signed the DoD Section 508 Policy Manual 8400.01- M, "Procedures for Ensuring the Accessibility of Electronic and Information Technology (E&IT) Procured by DoD Organizations." This document implements the policy in DoDD 8000.01, assigns responsibilities for Section 508 management, and provides procedures for the implementation of Section 508. The Manual may be found online at: http://www.dtic.mil/whs/directives/corres/pdf/840001m.pdf

The Office USD(AT&L), establishes DoD-wide policy for ensuring the accessibility of E&IT procured by DoD organizations in accordance with DoDD 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005. Additionally, the

USD(AT&L) names a Chief Acquisition Officer representative to work with the DoD Section 508 Coordinator in the Office of the DoD CIO toward DoD-wide implementation of Section 508.

Requiring Officials and Contracting Officers need to ensure that when developing solicitations for E&IT, reference is made to the E&IT accessibility standards as developed by the U.S. Access Board (36 CFR Part 1194) and incorporated in the FAR (Part 39.2).

(IXXC) The Office of the DoD Section 508 Coordinator has developed proposed Section 508 content for curriculum at the National Defense University's i-College and the Defense Acquisition University (DAU). Also under consideration for development, should funding be available, is a Section 508 webinar for DAU students. Additionally, the Department has developed and is working with GSA to conduct on-site and virtual training for Components with a high percentage of non-Section 508-compliant solicitation assessments. Over the course of these sessions, the DoD Section 508 Coordinator briefs DoD policy and guidance, and GSA gives a Section 508 Overview and conducts training on making solicitations compliant.

The CIO and Acquisition community may access any of the following links for assistance with developing solicitations for E&IT:

1. GSA's Guidance on Creating 508-Compliant IT Solicitations:

   http://buyaccessible.net/blog/wp-content/uploads/2011/01/Guidance-on-Creating-508-Compliant-IT-Solicitations.pdf

2. BuyAccessible Wizard at https://app.buyaccessible.gov/baw/, which includes recommended solicitation language for E&IT labor hours, in addition to E&IT products.

CIO Authorities Requirement Submission

As permitted by the PortfolioStat Deliverables email from the CIO Council, dated April 29, 2013, the DoD CIO submitted its response to OMB's CIO Authorities requirement (as stated in the OMB FY14 budget guidance) on MAX Portal, concurrently with the posting of the draft DoD IRM Strategic Plan.