DoD Enterprise Roadmap, 31 August 2012

BRIAN G. WILCZYNSKI
Director, Architecture & Interoperability
Office of the DoD CIO
Executive Summary
The Department of Defense (DoD) Enterprise Roadmap (ER) documents the Chief Information Officer’s approach toward developing, maintaining, and using architectures that support the strategic objectives of the Department. It discusses the overall DoD Enterprise Architecture (EA) and identifies performance gaps, resource requirements, planned solutions, transition plans, and a summary of the current and future architecture. The Department’s current focus is on the establishment of a Joint Information Environment (JIE) that will achieve efficiencies while improving operational effectiveness and cyber security posture. The Information Technology Enterprise Strategy and Roadmap (ITESR), approved by the Deputy Secretary in October 2011, established the high level goals for improving DoD’s information technology infrastructure. These goals are now being pursued in the architecting of the JIE by addressing network normalization, data center consolidation, identity and access management, enterprise services, and more effective governance.

The DoD is a complex organization comprising multiple Components (i.e., Combatant Commands, Services, and Agencies) whose missions and operations vary. These Components function autonomously and as interoperable, integrated elements. As a result, a single, monolithic DoD EA cannot effectively describe all the DoD Components; their current and future capabilities, functions, and relationships; or their various transition strategies. Instead, the DoD EA needs to provide an effective description of all DoD Components and relate them in a meaningful way.

To achieve this, the DoD has adopted a federated approach for developing and managing the DoD EA that is based on enterprise-level guidance, mission area, and Components architectures. A federated DoD EA is the best way to describe this complex Department effectively and provide the necessary context and guidance to govern, manage, and accomplish its missions. The DoD EA Federation Strategy\(^1\) describes an approach to enterprise architecture that facilitates interoperability and information-sharing between semi-autonomous military departments, components, and programs. This approach recognizes the need for autonomy, but requires linkages and alignment of architectures from the program level to the enterprise level.

Although the federated approach and structure for the DoD EA is constant, its content continues to grow and mature as new architectures are approved and existing ones are updated. In adherence to the Office of Management and Budget (OMB) guidance, the DoD has established Mission Areas to guide and support information technology investments and solutions. The DoD EA is used to guide investment portfolio strategies and decisions; define capability and interoperability requirements; establish and enforce standards; guide security and information assurance requirements across DoD; and provide a sound basis for transitioning from the existing environment to the future.

---
\(^1\) GIG Federation Strategy, signed 2007
# Table of Contents

1  Introduction .................................................................................................................. 1
  1.1  Purpose ......................................................................................................................... 1
  1.2  Content and Organization ............................................................................................. 1
  1.3  Intended Use .................................................................................................................. 1

2  Department of Defense Enterprise Architecture Management .................................... 2
  2.1  DoD Enterprise Architecture ......................................................................................... 2
  2.2  DoD Approach for Managing the Enterprise Architecture ........................................... 3
  2.3  Governance and Use ....................................................................................................... 4
    2.3.1  Business Mission Area Governance ........................................................................ 5
    2.3.2  Warfighting Mission Area Governance ................................................................... 5
    2.3.3  Defense Intelligence Mission Area Governance ..................................................... 5
    2.3.4  Enterprise Information Environment Mission Area Governance ........................... 5
    2.3.5  Component Governance ......................................................................................... 6
  2.4  Support for Strategy and Business ................................................................................. 6
  2.5  Enterprise Architecture Roles and Responsibilities ..................................................... 7
  2.6  Enterprise Architecture Program Budget ....................................................................... 8
    2.6.1  Department of Defense Architecture Framework .................................................... 8
    2.6.2  Department of Defense Architecture Registry System ........................................... 8
    2.6.3  Department of Defense Information Technology Portfolio Repository .................. 9
    2.6.4  Department of Defense Information Technology Standards Registry ................... 9
    2.6.5  Department of Defense Metadata Registry ............................................................. 9
    2.6.6  Interoperability and Supportability Assessment Module .......................................... 10
    2.6.7  Joint Common Systems Function List ..................................................................... 10
    2.6.8  Enhanced Information Support Plan ....................................................................... 11
    2.6.9  Global Information Grid Technical Guidance Framework ..................................... 11
  2.7  Enterprise Architecture Program Performance Measures ......................................... 11

3  Summary of Current Architecture .................................................................................... 13
  3.1  Strategic Goals and Objectives ..................................................................................... 14
  3.2  Identification of Services, Applications, Infrastructure and Standards ......................... 18
  3.3  Alignment to the OMB’s Common Approach to Federal EA ...................................... 18

4  Summary of Future Architecture ....................................................................................... 20
  4.1  Planned Modernization ................................................................................................. 20
    4.1.1  Enterprise Information Environment Mission Area Modernization ...................... 21
4.1.2 Warfighting Mission Area Modernization
4.1.3 Business Mission Area Modernization
4.1.4 Intelligence Mission Area Modernization
4.1.5 Component Modernization
4.2 Joint Information Environment (JIE)
4.2.1 Enterprise IT Infrastructure and Sub-functions
4.2.2 Vision
4.2.3 Alignment to the DIEA
5 Appendix 1: IT Asset Inventory
6 Appendix 2: Commodity IT Consolidation Plan
6.1 Agency COO Communication to the Agency
6.2 Executive Summary
6.3 Scope and Complexity
6.4 DoD Areas of Focus
6.5 IT Portfolio Management Overview
6.6 Commodity IT Consolidation Plan
6.7 Lessons Learned and On-Going Performance Measurement
7 Appendix 3: Line of Business Service Plan
8 Appendix 4: IT Shared Service Plan
8.1 Unclassified Information Sharing Service/All Partner Access Network (UISS/APAN)
8.2 General Fund Enterprise Business System (GFEBS)
9 Appendix 5: Key Artifacts for the Department of Defense Enterprise Architecture
10 Appendix 6: Acronyms
List of Figures
Figure 1. Department of Defense Enterprise Architecture Graphic ........................................... 3
Figure 2. Enterprise Architecture Management Approach ......................................................... 4
Figure 3. Enterprise Architecture Outcomes and Required Elements ........................................ 12
Figure 4. DoD Taxonomy for Program Alignment ...................................................................... 19
Figure 5. Joint Information Environment End-State .................................................................... 27
Figure 6. Joint Information Environment Increment Planning ...................................................... 27
Figure 7. Joint Information Environment Alignment with DIEA .................................................. 28

List of Tables
Table 1. Department of Defense Enterprise Architecture Roles and Responsibilities ............ 7
Table 2. Department of Defense Enterprise Architecture Enablers .......................................... 9
Table 3. Department of Defense CIO Strategic Goals and Objectives ................................... 14
Table 4. Enterprise Information Environment Mission Areas Modernization .......................... 21

Table E-1. Key Information about the Department of Defense Enterprise Architecture .......... 59
1 Introduction

The Office of Management and Budget (OMB) Common Approach to Federal Enterprise Architecture (FEA) and the OMB memorandum, Subject: Increasing Shared Approaches to Information Technology Services, dated May 2, 2012, require each Federal Agency Chief Information Officer (CIO) to submit an “Enterprise Roadmap” annually to support the Federal Budget process and to ensure information technology (IT) shared services are implemented in a coordinated and expedited manner. The Common Approach to FEA (CAF) provides detailed guidance for information that should be described in the Enterprise Roadmap, and the OMB memorandum describes additional appendices that should be included. The DoD Enterprise Roadmap adheres to the guidance provided by both documents.

1.1 Purpose

The DoD Enterprise Roadmap (Roadmap) documents and maps the DoD’s strategic goals to business services, integrating technology solutions across all DoD Mission Areas (i.e., Warfighting, Business, and Defense Intelligence). The Roadmap documents the Chief Information Officer’s approach toward developing, maintaining, and using architectures that support the strategic objectives of the Department. The Department’s current focus is on the establishment of a Joint Information Environment (JIE) that will achieve efficiencies while improving operational effectiveness and cyber security posture. This living document will be updated at regularly and submitted annually to the OMB’s Office of e-Government and IT.

1.2 Content and Organization

In describing the transformation of the DoD, the Roadmap discusses the overall Enterprise Architecture (EA); identifies performance gaps, resource requirements, planned solutions, and transition plans; and summarizes the current and future architecture. The Roadmap also describes the DoD EA governance process, implementation methodology, and documentation framework. This content is organized to provide a logical progression of information and facilitate understanding. The three primary sections for organizing content are Enterprise Architecture Management, Current Architecture Summary, and Future Architecture Summary. Transition information is described in the Future Architecture Summary section. The document also contains four appendices that provide the IT Asset Inventory, Commodity IT Consolidation Plan, Line of Business Service Plan, and IT Shared Service Plan.

1.3 Intended Use

The DoD Enterprise Roadmap is intended to support the annual Federal Budget process and to serve as a DoD authoritative reference for IT portfolio reviews and program-level analysis and planning. It is also intended to guide the incremental transformation of the DoD as it progresses toward future target states.
2 Department of Defense Enterprise Architecture Management

The DoD EA is the description of the Department in terms of its mission goals, key organizational and functional components, and the inter-relationships among these components. This section describes the DoD EA and documents the activities associated with managing and administering the EA as an ongoing program. At a strategic-level, it addresses governance and use, support for strategy and business, EA roles and responsibilities, EA program budget, and EA performance measures. The DoD EA Management Plan (EAMP), currently under development, provides additional detailed descriptions about managing the DoD EA.

2.1 DoD Enterprise Architecture

As required by the OMB Circulars A-11 and A-130, the DoD maintains a target EA that is dynamic, changing, and expanding. Rather than being a single, overarching artifact, the target EA is a federation of architecture descriptions that provide context and rules for accomplishing the Department’s mission. Constituent architectures are developed and maintained at the Mission Area (MA) and Component levels to collectively define the people, processes, and technology required in the current and target environments. Each “subsidiary” architecture also provides a roadmap for transitioning a given part of the DoD to a new and improved target operating environment.

Figure 1 depicts the DoD EA, which comprises the functional and organization architectures. The EA looks at specific functions and capabilities, indicates what policies apply, and provides interpretation by highlighting the applicable policies and removing ambiguity through operational context. Using the DoD EA, decision-makers can look across the enterprise for gaps and for consolidation and shared service opportunities. The DoD EA will continue to institutionalize consistent and effective use of architecture across the Department and strengthen the use of architecture in the Department’s key decision-making processes. This includes the Joint Capabilities Integration and Development System (JCIDS); Defense Acquisition System (DAS); Business Capability Life-cycle (BCL); Planning, Programming, Budgeting and Execution (PPBE); Capability Portfolio Management (CPM); and Joint Concept Development and Experimentation (JCD&E).

The DoD EA is a federated system in which the leadership of each MA (Warfighting, Business, Intelligence, and Enterprise Information Environment) and Component (e.g., military department, defense agency, and combatant command) maintains its own architectural documentation and transition plan, and coordinates with all entities with which it overlaps and shares services and capabilities. Each effort is substantial in itself. Enterprise rules outline how the parts of the federation interrelate to affect optimal Department-wide performance. Each mission area and component transition plan is very dynamic with widely ranging periodicity, depending upon need.

The four MAs in the top half of Figure 1 are enterprises unto themselves that collectively represent the operational and supporting missions of the Department. Each MA has an EA that describes the concepts, principles, rules, activities, and services associated with the MA.
The DoD Components, shown in the bottom half of Figure 1, represent enterprises unto themselves, operating within the scope of the larger DoD enterprise. Each Component has EAs that align with the MA architectures and interoperate with architectures maintained by each of the other Components to support DoD missions jointly.

The bottom row of Figure 1 shows the architecture tools, reference models, standards, guidance, and the laws, regulations, and policies that guide, govern, and support architecture development, management, and use. These are reflected in the DoD EA as controls on the business processes, business activities, business rules, IT services, IT standards applied, and information/data handling throughout the Department.

2.2 DoD Approach for Managing the Enterprise Architecture

The approach for managing the DoD EA is threefold: 1) provide enough guidance to direct and steer the Mission Areas and Components toward the DoD EA vision; 2) provide ample flexibility and agility for the Mission Areas and Components to develop their aspects of the DoD EA through a federated approach using “just enough” and “just in time” principles in incremental development; and 3) provide an oversight and compliance functions in an efficient manner by requiring that a minimal set of criteria be self-assessed by a limited number of stakeholders (i.e., Mission Areas, Military Components, Services, and some Agencies).

The threefold approach is translated into three layers of guidance and oversight (see Figure 2) that are described by: the EA Drivers (laws, regulations, and policies) that drive the development and use of architecture; EA Management, which guides and steers the transition of the current
baseline of the DoD EA to its vision; and EA Use, which influences and spurs the incorporation of DoD EA content into the analysis and discussion prior to making decisions.

Figure 2. Enterprise Architecture Management Approach

An important concept for managing and governing the DoD EA is “tiered accountability.” Tiered accountability aligns responsibility for development, management (including governance), and execution of the DoD EA across the Department, Mission Areas, and Components.

2.3 Governance and Use

Governance involves the planning, decision-making, and oversight processes and people that determine how the EA is developed, verified, versioned, used, and sustained over time. Each Mission Area and Component is responsible for establishing its own governance body and processes in accordance with associated guidance and the DoD EAMP. Components also participate in Mission Area governance processes, as they apply to the architecture or solution being developed. For example, Army architecture for a personnel system/service/process must participate in the Army governance process and the Business Mission Area governance process.

Each governance body is guided by its charter, which is reviewed annually. The charter defines the purpose for the body, lists its objectives, states the level of authority given to the body to make decisions, and defines the roles and responsibilities of the membership.

Policies and guidance documents serve as inputs and controls for the activities performed by the governance processes. The governance processes for the Mission Areas and Components are at varying degrees of maturity; the Business Mission Area is the most mature.
2.3.1 Business Mission Area Governance
The content for this section will be available in future document releases.

2.3.2 Warfighting Mission Area Governance
The Joint Staff is the primary organization for the Department’s warfighting mission. It has developed and implemented the JCIDS process as its primary means of prioritizing and managing investments, including IT and National Security Systems. The JCIDS process is driven by strategic direction, input from the Combatant Commands in the form of Integrated Priority Lists, and input from the Joint Requirements Oversight Council by way of Joint Requirements Oversight Council Memorandums. The outputs from the JCIDS process and Joint Staff guide the management decisions for when systems are procured.

2.3.3 Defense Intelligence Mission Area Governance
The content for this section will be available in future document releases.

2.3.4 Enterprise Information Environment Mission Area Governance
The DoD EA is used to guide the Department’s performance improvement with a focus on four key elements:

- Define, develop, and maintain enterprise architecture. The Department maintains the DoD EA at the enterprise and component levels while ensuring that the overarching structure for federating architectures aligns to the DoD’s portfolio structure. The DoD EA is used to ensure that investments are properly assessed in a federal-wide context by aligning all information technology investments with the FEA Reference Models and the Common Approach to Federal Enterprise Architecture.

- Define, develop, and maintain solution architectures. The Department develops and maintains solution architectures for material and non-material initiatives and capabilities that deliver functionality for the DoD information enterprise, ensuring that both the solution architectures and solutions conform to the DoD EA.

- Use DoD architecture information for better-informed decisions. The Department uses the DoD EA to guide investment portfolio strategies and decisions, define capability and interoperability requirements, establish and enforce standards, guide security and information assurance requirements across DoD, and provide a sound basis for transitioning from the existing environment to the future. In addition, DoD EA guides solution architectures to clearly articulate requirements, influence design and implementation, and demonstrate interoperability. It is also used to review all IT investments, including those related to National Security Systems, for compliance with the DoD EA and applicable approved solution architectures. The DoD EA institutionalizes consistent and effective use of architecture across the Department and strengthens the use of architecture in the Department’s key decision-making processes, including JCIDS, DAS, BCL, PPBE, CPM, and JCD&E.

- Govern the DoD EA. The Department governs architectures through formal processes consistent with its organizational and functional structure. Using these formal governance processes, architectures will be registered and approved, and the DoD will continue to sustain
and apply standards for documenting architecture content to promote reuse, common vocabulary, and integration.

The Department conducts periodic assessments of architecture management maturity and the contributions of architecture to mission effectiveness, efficiency, information-sharing, and transparency. The DoD CIO has reorganized the governance structure to align with emerging policy better.

The Architecture and Standards Review Group (ASRG) is the primary governance body responsible for architectures and standards. The ASRG, which has DoD-wide membership, is responsible for recommending approval of architectures for inclusion in the architecture federation or DoD EA. It also is responsible for approval of IT standards for inclusion in the DoD Information Technology Standards and Profile Registry (DISR). The ASRG and two other review groups, the Enterprise Services Review Group and Information Assurance Enterprise Review Group, perform governance functions as part of a larger CIO Executive Board (ExBd).

One ExBd’s objective is to develop and approve enterprise-wide guidance (including architecture, standards, and policies) for determining effectiveness or identifying deficiencies (with resulting courses of action) in satisfying DoD mission needs. To achieve this, the ExBd:

- Guides the development of the DoD EA and related policies and standards.
- Approves enterprise information architectures, policies, and standards to guide and support the management of DoD IT within PPBE (including CPM and Capital Planning and Investment Control), and JCIDS and DAS processes.
- Approves enterprise-wide guidance and tool requirements to support IT analysis and management across the Department by Component CIOs, Component Acquisition Executives, IT Portfolio Management (PfM) Mission Area Leads, and DoD CPM Co-Leads.
- Tasks tiger teams to research specific issues related to enterprise architecture and IT implementation strategies in a collaborative, transparent, and objective manner. Uses tiger team reports to frame enterprise guidance.
- Assesses the technical, operational, and financial costs and benefits of potential enterprise services, providing a process by which potential enterprise services can be reviewed and approved for designation as Mandatory Core DoD Enterprise Services and/or Shared DoD Enterprise Services.

### 2.3.5 Component Governance

The content for this section will be available in future document releases.

### 2.4 Support for Strategy and Business

Emphasizes that one of the main purposes of the EA program is to support and improve the Enterprise’s strategic and business planning and to identify performance gaps that architectural designs can help close.
2.5 Enterprise Architecture Roles and Responsibilities

The roles and responsibilities described in this section are necessary to ensure consistent management, development, and use of the DoD EA and its parts. Table 1 describes these roles and responsibilities.

<table>
<thead>
<tr>
<th>ROLES</th>
<th>RESPONSIBLE ORGANIZATION</th>
<th>RESPONSIBILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoD Chief Architect</td>
<td>DoD CIO</td>
<td>• Establish the policy, standards, and guidance to enable the consistent management of EA within each MA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Establish the requirements and processes for performing cross-mission IT portfolio analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Provide cross-mission IT portfolio recommendations to senior leadership</td>
</tr>
<tr>
<td>Mission Area (MA) Chief Architect</td>
<td>JCS J6, DCMO, USD(I), and DoD CIO/DISA</td>
<td>• Develop and maintain the EA for the MA</td>
</tr>
<tr>
<td>(Warfighting, Business, Intelligence, and EIE)</td>
<td></td>
<td>• Support the governance and use of the MA EA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Manage and maintain MA standards and guidance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Provide MA investment recommendations to senior leadership</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Coordinate MA-related dependencies with other MA chief architects</td>
</tr>
<tr>
<td>Component Chief Architect</td>
<td>Army, Navy, Air Force, NSA, etc.</td>
<td>• Develop and maintain the EA for the Component</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure alignment with relevant MA architectures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Manage and maintain Component standards and guidance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Provide Component investment recommendations to senior leadership</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Coordinate dependencies among other Components architectures</td>
</tr>
<tr>
<td>Architecture Community Steward</td>
<td>All</td>
<td>• Develop and manage architecture development frameworks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Provide tools that facilitate the discovery and reuse of architecture data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Foster outreach and architecture workforce development</td>
</tr>
</tbody>
</table>
2.6 Enterprise Architecture Program Budget

The overall budget for developing and managing the DoD EA consists of the combined budgets for each MA and Component that is part of the DoD EA. Implementing a federated EA is very complex. Future document releases will contain general projected budget information for MAs and Components for the following three years.

The DoD EA also contains a common set of tools and programs that are used by all elements in developing, implementing, and managing the DoD EA. They include the DoD Architecture Framework (DoDAF), DoD Architecture Registry System (DARS), DoD Information Technology Portfolio Registry (DITPR), DoD Information Technology Standards Registry (DISR), DoD Metadata Registry (MDR), Interoperability and Supportability Assessment Module (IAM), Joint Common Systems Function List (JCSFL), Enhanced Information Support Plan (EISP), and Global Information Grid Technical Guidance Framework (GTG-F). A short description of these tools and programs is provided in the following paragraphs and represented in Table 3.

2.6.1 Department of Defense Architecture Framework

The DoDAF serves as the overarching, comprehensive framework and conceptual model for the development of architectures that enable DoD managers at all levels to make key decisions more effectively through organized information-sharing across the Department, Mission, Component, and Program boundaries. It is the Department’s means for standardizing representation of architecture information.

The DoDAF serves as one of the principal pillars supporting the DoD CIO in his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. It also reflects guidance from the OMB Circular A-130 and other Departmental directives and instructions. The DoDAF has been coordinated with the development of the OMB Common Approach resulting in a direct mapping to the Common Approach core artifacts. The DoDAF and the Common Approach will continue to align as further documentation guidance is developed. The current version, DoDAF V2.0, focuses on architectural data. In general, data can be collected, organized, and stored by a wide range of architecture tools developed by commercial sources.

The DoD promotes the adoption, use, and exchangeability of DoDAF architectures through standardization efforts. The DoD works with tool vendors in organizations such as the Object Management Group and the International Organization for Standardization. It also works with Allied and other countries on a next-generation framework, the Unified Architecture Framework, based on DoDAF 2. The long-term vision is developing a set of common, commercial supporting tools suitable for use internationally and nationally. This is based on a further refinement of generic and standardized architecture ontology (data models).

2.6.2 Department of Defense Architecture Registry System

The DoD uses the DARS to register and catalog all DoD architectures to provide architecture discoverability and accessibility across the Department. It provides a visualization of the federated DoD EA and a means to federate and link architectures to enterprise reference models and segment architectures.
2.6.3 Department of Defense Information Technology Portfolio Repository

The DoD Information Technology Portfolio Repository (DITPR) and the DoD Secure Internet Protocol Router Network (SIPRNet) IT Registry are the Department’s authoritative inventories of IT systems. They provide senior DoD decision-makers with: 1) a coherent and contextual view of the capabilities and associated system enablers for making resource decisions; and 2) a common central repository for IT system information to support the certification processes of the various Investment Review Boards and the Defense Business Systems Management Committee.


2.6.4 Department of Defense Information Technology Standards Registry

The DISR is an online repository of IT standards, formerly captured in the Joint Technical Architecture, Version 6.0. The DISR supports the continuing evolution of the DISR and the automation of all its processes. It is also the repository for information pertaining to National Security Systems standards. DISR standards are to be used within DoD as the “building codes” for all new systems. They are intended to facilitate interoperability and integration of systems within the Global Information Grid (GIG). DISR also provides the ability to specify profiles of standards that programs will use to deliver net-centric capabilities.

Table 2. Department of Defense Enterprise Architecture Enablers

<table>
<thead>
<tr>
<th>EA Tools and Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoD Architecture Framework (DoDAF)</td>
</tr>
<tr>
<td>DoD Architecture Registry System (DARS)</td>
</tr>
<tr>
<td>DoD Information Technology Portfolio Registry (DITPR)</td>
</tr>
<tr>
<td>DoD Information Technology Standards Registry (DISR)</td>
</tr>
<tr>
<td>DoD Metadata Registry (MDR)</td>
</tr>
<tr>
<td>Interoperability &amp; Supportability Assessment Module (IAM)</td>
</tr>
<tr>
<td>Joint Common Systems Function List (JCSFL)</td>
</tr>
<tr>
<td>Enhanced Information Support Plan (EISP)</td>
</tr>
<tr>
<td>Global Information Grid Technical Guidance Framework (GTG-F)</td>
</tr>
</tbody>
</table>

2.6.5 Department of Defense Metadata Registry

As part of the overall DoD Net-Centric Data Strategy, the DoD CIO established the DoD MDR and a related metadata registration process for the collection, storage, and dissemination of structural metadata information resources (e.g., schemas, data elements, attributes, document type definitions, style-sheets, data structures). This Web-based repository also acts as a clearinghouse through which industry and government coordination on metadata technology and
related metadata issues can be advanced. As the Executive Agent of the Office of the Assistant Secretary of Defense, the Defense Information Systems Agency (DISA) maintains and operates the DoD MDR under the direction and oversight of DoD CIO.

2.6.6 Interoperability and Supportability Assessment Module

Capability document assessments are conducted at each program milestone to ensure that interoperability and supportability requirements are addressed throughout the life-cycle of DoD IT and National Security Systems. The IAM, as part of the GIG Technical Guidance (GTG) Foundation, performs these document assessments. The IAM service provides a collaborative assessment environment for staffing, reviewing, and adjudicating structured Information Support Plan (ISP) and GIG Technical Profile (GTP) data. Real-time collaboration occurs within the assessment community to achieve Interoperability and Supportability certification. The IAM is used to:

- Develop, support, and enforce key enablers of end-to-end life-cycle interoperability and supportability by ensuring the use of DoD IT Standards, analysis of system interoperability, interconnectivity, and architecture availability to facilitate information-sharing throughout DoD.
- Assess and analyze capability documents for Interoperability and Supportability requirements in accordance with DoD and Joint Staff J6 policy.
- Act as the DISA focal point for the Interoperability and Supportability assessment and analysis of all DoD programs.

The IAM replaces the former Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool–Empowered (JCPAT-E).

2.6.7 Joint Common Systems Function List

The JCSFL is a catalog of common system functions providing a common lexicon of functionality performed by systems and services that support warfighting capabilities across the Joint force. The JCSFL is used in the development of DoDAF integrated architectures, JCIDS capability description documents, ISPs, and their supporting solution architectures products. Use of the JCSFL in integrated architectures enables horizontal and vertical assessment of capabilities and systems. The Joint Staff J6 Deputy Director for Command and Control Integration, Architecture and Integration Division maintains the JCSFL, coordinates the integration of new functionality submitted by the military service systems commands and capability developers, and assists architects to ensure compliance requirements for its use are satisfied.

The Manual for the Operations Joint Capabilities Integration and Development System, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01 (series)-Net-Ready Key Performance Parameter (NR-KPP), and the supporting NR-KPP Manual require that architecture products align to the JCSFL. Compliance is achieved by direct use of the JCSFL functions, as named and defined in the JCSFL Dictionary, or by translating domain-specific system functions to the JCSFL functions in a crosswalk. The crosswalk method permits architects to comply with the requirement to use the JCSFL, but not inhibit the use of domain-specific language needed to drive lower-level requirements.
2.6.8 Enhanced Information Support Plan

The Enhanced Information Support Plan (EISP) tool is used to fulfill the requirements for creating an ISP or Tailored Information Support Plan. It assists ISP developers through a series of pre-defined fields that center on the analysis of a program’s processes, operational activities performed to complete a mission, and critical information needs (e.g., data and information passed between users through supporting systems that enable mission completion). The structured data collection template in the EISP tool ensures only the required essential information is entered. It also assists in showing compliance with policies and instructions.

The EISP tool evolves the ISP process from “document-centric” to “data-centric.” It provides a streamlined process for collecting, reviewing, and reusing data. In addition, it is an efficient approach for data collection that builds the mandated document while guiding the analysis of the data as it is entered.

2.6.9 Global Information Grid Technical Guidance Framework

The DoD CIO, in partnership with DISA, has developed and instituted the GTG-F to create a more efficient and effective interoperability assessment process. The GTG-F is hosted on the DISA Defense Enterprise Computing Center and driven by the EISP, enabling compliance with the DoD Information Enterprise Architecture (IEA), GIG Technical Profiles (GTP), and DISR IT standards. The data captured within the EISP and GTP module is pushed to the Interoperability Assessment Module, which provides a streamlined staffing, review, and commenting process for interoperability data. The GTG-F enables Program Managers (PM) to identify interoperability risks and issues better and to develop mitigation plans with online templates, business rules, and data validation capabilities.

2.7 Enterprise Architecture Program Performance Measures

The effectiveness and efficiency of the DoD EA program is measured in terms of outcome and output. The three expected outcomes for the DoD EA are:

- Improved IT Investment Decision-Making
- Increased Interoperability
- Realization of e-Government and Paperwork Reduction.

A sound foundation of data, processes, and tools must be in place to achieve the outcomes of EA. Data consists of the information elements needed to achieve the outcome. Processes provide the mechanism to manage, maintain, analyze, and apply the information. Tools facilitate the process and actual use of the information. Supporting all of these elements is governance. Governance ensures that outcomes remain relevant; data, processes, and tools continue to target accomplishment of the outcome; and outcomes are success.

Figure 3 identifies the key elements of each Title authority-driven, EA outcome. Some elements apply across outcomes, but are individually identified for clarity. These elements do not focus on the development of architecture, nor are they considered architecture products. The focus in establishing these elements is to capture the right information and enable the use of that information in making decisions that support the enterprise.
Figure 3. Enterprise Architecture Outcomes and Required Elements

**For Official Use Only**
3 Summary of Current Architecture

This section summarizes the linkage between current services and the resources involved in providing the services in each area of the DoD EA. The objective is not to duplicate extensive documentation, but to provide an integrated view of current business activities and supporting technology solutions. The current DoD EA is comprised of architecture descriptions of four MAs and Components.

The DoD Enterprise Architecture (EA) is a federation of Mission Area, component, and solution architectures developed using policy, guidance, and tools provided by the enterprise. The following are key elements comprising the current DoD EA.

- DoD Information Enterprise Architecture (IEA), v2.0, July 2012: Approved on 10 August 2012. The IEA currently includes a series of enterprise wide Reference Architecture, as described in the Reference Architecture Descriptions (RADs). The RAD was released under approval of the ASRG in June 2010.
  - Core Data Center (CDC) RA: Expect approval in September 2012
  - Unified Capabilities (UC) RA: Expect approval in September 2012
  - Network Optimization RA (NORA): Expect approval in CY12

- Business Enterprise Architecture (BEA), Version 9.0: Published on 16 April 2012

- Joint Information Environment Operational Reference Architecture (JIE ORA), Version 1.0, September 2011: Approved on 17 November 2011

- Defense Intelligence Information Enterprise – Framework (DI2E-F): Currently under development

- Army Enterprise Architecture (AEA): Currently under development

- DON Enterprise Architecture, Version 3.1, 14 September 2011: Released on 2 April 2012

- Air Force Enterprise Architecture (AFEA), Version 3.6: Released on 10 Jan 2011

- Reference Architecture (RA) Description, June 2010: Approved in June 2010

Per the OMB Common Approach to FEA (CAF), future versions of the DoD Enterprise Roadmap will address all MAs and key Components and provide information in the following areas:

- Strategic Goals and Initiatives—Identifies strategic goals and how the EA program and specific resources support attainment of these goals.

---

For Official Use Only

- Business Services and Information Flows—Identifies and emphasizes the role that EA plays in supporting business process analysis and improvement, and identifying and optimizing information flows within and between these processes.

- Applications—Identifies how current EA artifacts at the applications-level support the information flows required for program activities throughout the DoD.

- Infrastructure—Discusses voice, data, video, and mobile hosting environments that make up the infrastructure level of the EA.

- Security and Privacy—Discusses the general approach to IT security and data privacy. Provides high-level descriptions on how security is built into business services and the control of information flow.

- Standards—Documents the business standards for mission and support services, and the technical standards for systems applications and infrastructure.

- Workforce Requirements—Describes required changes to knowledge and skill requirements.

For the August 2012 submission, the DoD Enterprise Roadmap will focus on the MAs by describing their current strategic goals and objectives, and the services, applications, infrastructure, and standards associated with achieving these goals.

3.1 Strategic Goals and Objectives

Table 3 describes the strategic goals and objectives for the EIEMA, as defined in the DoD CIO Campaign Plan.

Table 3. Department of Defense CIO Strategic Goals and Objectives

<table>
<thead>
<tr>
<th>Mission Area</th>
<th>Goals</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIE</td>
<td>AOE 1: Provide Enterprise Policy and Architecture - Provide enterprise policy and architecture within and appropriate governance framework to guide the development and delivery of secure, integrated information capabilities necessary for mission success</td>
<td>PRI 1.1: Develop CIO Policy Framework - Development of the policy framework to oversee and manage the DoD Information Enterprise (as defined in DoDD 8000.01). PRI 1.2: Evolve the DoD Enterprise Architecture (EA) and Processes - Consolidate and refine existing DoD EA descriptions, governance, processes, and federation requirements into architecture policy and an overarching Enterprise Architecture Management Plan (EAMP) that institutionalizes DoD-wide use of and compliance with the DoD EA. PRI 1.3: Strengthen CIO Governance - Update the governance structure, policy, and processes to guide and oversee the development and evolution of the DoD Information Enterprise to meet customer needs and strategic objectives.</td>
</tr>
</tbody>
</table>

3 Department of Defense (DoD) Chief Information (CIO) Campaign Plan, Baseline 0, 5 October 2011
<table>
<thead>
<tr>
<th>Mission Area</th>
<th>Goals</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOE 2: Drive Secure IT Infrastructure and Services - Drive IT infrastructure and services that support an agile force by providing secure access to the information needed to perform their missions—anywhere, anytime.</td>
<td>PRI 2.1: Optimize the IT Infrastructure through Consolidation efforts and by Providing Common Services - Consolidate IT infrastructure under common IT services to enable DoD to manage infrastructure as a commodity. PRI 2.2: Integrate Network Transport Capabilities - Ensure the integration, interoperability, and synchronization of information transport capabilities in the space, aerial, terrestrial, maritime, and cyberspace domains through participation in the Joint Capabilities Integration Development System (JCIDS); Planning, Programming, Budgeting, and Execution (PPBE); and Defense Acquisition System (DAS) processes. PRI 2.3: Enable Secure Information Sharing - Enable all authorized users to have immediate, secure, and reliable access to the information they need to perform their missions and support effective and agile decision making. PRI 2.4: Deploy Enterprise Services - Implement a suite of DoD enterprise services accessible by authorized users anywhere, anytime, while stationary and mobile, from tactical edge to sustaining base. PRI 2.5: Implement Identity and Access Management - Provide timely access to information using authentication infrastructure that provides Dynamic Access Control capabilities granting authorized users access to information assets based on established enterprise identity attributes that contain biographical, contextual, and biometrics data. PRI 2.6: Transition to Cloud Computing Environment - Drive delivery and adoption of a secure, dependable enterprise cloud computing environment to enhance mission effectiveness and improve IT efficiencies to meet mission needs and support anywhere, anytime, information access. PRI 2.7: Manage Spectrum - Ensure DoD Spectrum access to meet warfighting needs. PRI 2.8: Ensure National Leadership Command Capabilities (NLCC) Assured Connectivity - Provide a robust DoD process and vision for producing assured, reliable, and enduring national-level command, control, and communications capabilities utilizing a set of secure and non-secure National Leadership Command Capabilities information services and information environment PRI 2.9: Improve Joint C2 Capabilities - Provide</td>
<td></td>
</tr>
</tbody>
</table>
### Mission Area | Goals | Objectives
--- | --- | ---
**AOE 3: Forge Partnerships** - Form collaborative partnerships with internal and external stakeholders to deliver responsive mission essential capabilities, protect DoD equities, and ensure interoperability and reliability—by aligning strategic plans, architecture, and standards; balancing capital investments; and integrating doctrine and operational procedures.  
**PRI 3.1: Foster More Effective Partnerships at the Federal, State, Local, and Tribal Levels** - Ensure that partnerships with key federal, state, local, and tribal government organizations provide more timely situational awareness for decision makers and enable trusted collaboration.  
**PRI 3.2: Establish Clear Roles and Responsibilities with DoD and Non-DoD Partners on NLCC Support** - Strengthen and clarify DoD CIO partnerships with COCOMs, Military Services, and Agencies, and create governance structures with clear strategies, priorities, accountability, and metrics.  
**PRI 3.3: Ensure Warfighters Receive Appropriate DoD CIO Support for Contingency Operation ICT** - Strengthen existing relationships and establish new processes/procedures to ensure ICT issues for the Warfighter that require DoD CIO involvement are visible and receive priority action for resolution, through partnerships with COCOMs, Military Services, and Agencies, and create governance structures with clear strategies, priorities, accountability, and metrics.  
**PRI 3.4: Enable Information Sharing and Secure Collaboration with NATO and Other Key Allies and Partners to Support Our Mutual Defense Interests** - Strengthen existing international relationships and guide DoD CIO cooperation activities based on goals and policy specific to activity, functional area, or nation.  
**PRI 3.5: Enhance DoD CIO Strategy and Communications** - Improve alignment of DoD CIO organizational responsibilities with our mission 1563 partners.  
---
**AOE 4: Evolve the IT Workforce** - Develop and sustain a broader, balanced current workforce and “workforce of the future” with the competencies and proficiencies necessary to operate, defend, and advance the  
**PRI 4.1: Manage the IT/Cybersecurity Functional Community Workforce** - Apply the FCM framework for effective strategic planning and workforce sustainment.  
**PRI 4.2: Strengthen the IT Acquisition Workforce** - Establish, maintain, and manage the IT Acquisition career field competency model; certification standards; career paths; and position category descriptions.  
**PRI 4.3: Enhance IT/Cybersecurity Recruiting and Retention, Education, Training, and Professional
<table>
<thead>
<tr>
<th>Mission Area</th>
<th>Goals</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoD IE.</td>
<td>Development - Recruit and retain, educate, train, certify, and continually develop opportunities to support a highly-qualified IT/cybersecurity workforce.</td>
<td>PRI 5.1: Manage the IT Budget - To improve IT investment planning, programming, and budget processes to better oversee IT investment execution by enhancing the framework and processes for decision making on future programs. PRI 5.2 Enhance the IT Acquisition Process - To enhance IT acquisition process to more effectively manage the Department's investments in technologies, programs, and product support. PRI 5.3: Enhance IT Portfolio Management Tools - Leverage tools and processes to support the management of the DoD IT portfolio. PRI 5.4: IT Investment Oversight - To provide guidance for and perform the DoD CIO investment oversight role. PRI 5.5: Support the Joint Information Environment - Provide necessary support to develop the JIE Resource Baseline.</td>
</tr>
<tr>
<td>AOE 5: Direct and Oversee DoD IT Investments - Optimize the Department's IT investments in infrastructure, business systems, weapons systems, communications, and platforms to ensure mission success and efficient use of resources</td>
<td>PRI 6.1: Dependable Mission Execution in the Face of Cyber Warfare - Ensure networks and systems are designed, built and operated with mission assurance in mind. Commanders must be able to count on systems and information being available when needed, even in the face of cyber warfare by a capable adversary. PRI 6.2: Better, Agile, Safe Sharing Objective - Sharing with whatever partners a mission requires can be established quickly and safely, and ensuring that the sharing is sufficiently rich that mission execution is effective. PRI 6.3: DoD and Its Mission Partners Can Keep a Secret - Military missions require the ability to generate information, make plans, and take actions, all in a way that an adversary cannot see. Information, regardless of classification, must be protected at the appropriate level from improper disclosure or being compromised by an adversary. PRI 6.4: Give Mission Commanders Freedom of Action in Cyberspace - The large, shared infrastructures that DoD uses (NIPRNet, SIPRNet and JWICS) often let the mission risk assumed by one commander spill into the missions of other commanders. This cybersecurity priority is focused on</td>
<td></td>
</tr>
</tbody>
</table>
### 3.2 Identification of Services, Applications, Infrastructure and Standards

The strategic goals and objectives described in Table 3 are achieved with services, applications, infrastructure, and standards resources. There is a hierarchical relationship among these elements where standards support infrastructure, applications, and services; infrastructure supports applications and services; applications support services; and services provide for the realization of the objectives and goals. Table 5 identifies the services, applications, infrastructure, and standards needed to achieve the MA goals and objectives.

Future document releases will contain inventories of Services, Applications, Infrastructure and Standards in alignment to the Objectives represented in Table 4.

### 3.3 Alignment to the OMB’s Common Approach to Federal EA

All DoD Components are required to align each IT investment to the DoD EA Segment and FEA Business Reference Model (BRM). IT investments are aligned based upon which predominant function the IT investment (system) enables, and not upon what business areas they support. All DoD EA segments have been approved by OMB. The taxonomy used by DoD programs as defined by the Deputy CIO, Resources⁴ to align with the FEA BRM is documented in Figure 4.

---

⁴ DOD CIO Memorandum, 30 July 2012, Subject: OSD Guidance for FY 2014 Information Technology Budget Submissions
Figure 4. DoD Taxonomy for Program Alignment
4 Summary of Future Architecture

This section describes the plans in terms of modernization and progress. The goals and objectives discussed in Section 3 are still the basis for the DoD goals as we move forward. Alternative operating scenarios will be considered to determine when goals and objectives should change. This will change transition plans and roadmaps. Per the OMB Common Approach to FEA (CAF), future versions of the DoD Enterprise Roadmap will address all MAs and key Components and provide information in the following areas:

- Future Operating Scenarios—Describes future operating scenarios with a narrative description of purpose and scope. Discusses built-in planning assumptions and selected courses of action.
- Planning Assumptions—Provides a detailed discussion of the planning assumptions introduced in the Future Operating Scenarios in terms of what they mean to the priorities of the Department as it implements the future EA. The assumptions identify new capabilities and resources that will be needed to be successful in each scenario.
- Updating Current and Future Architecture Views—Documents planned changes in processes and resources. It begins with descriptions of strategic goals and initiatives at each level of the framework (Strategic Plans, Business Activities/Services, Data/Information Flows, Systems and Applications, and Networks and Infrastructure).
- Modernization—Documents the tasks, milestones, and timeframe for implementing new systems and services.
- Configuration Management—Serves to support the sub-process by which changes to the EA are managed and standards are applied.

For the August 2012 submission, the DoD Enterprise Roadmap will focus on the MAs by describing the modernization that is planned for the future.

4.1 Planned Modernization

The DoD EA continues to evolve to meet the future needs of the Department and provide forward-looking guidance. This evolution occurs as DoD EA references are updated, new architectures are developed, and existing architectures are refined. The Secretary of Defense sets the strategy, provides oversight, and manages capability integration across all DoD Components. Because each Component has its own business style, constituencies, and appropriations, it is essential that Components maintain responsibility for executing their assigned missions, conducting joint operations, and ensuring information flows freely across the enterprise.

The Department’s approach to net-centric transformation in this environment is guided by the concepts of tiered accountability and federation. Tiered accountability aligns responsibility for decision-making and execution across the tiers of the Department—DoD Enterprise, Component, and Program. Federation ensures decision-makers and implementers understand and align programs and capabilities across tiers. A federated approach allows each tier (in accordance with its Title authority) to leverage the decisions and services of other tiers. Each tier governs its area or responsibility. In addition, it should acknowledge and maintain consistency with the guidance from higher tiers. To improve understanding across all tiers, the DoD enterprise-level architectures depict Department-wide rules and constraints. The Component-level architectures
depict mission-specific services and capabilities. The program-level architectures depict solutions that conform to higher tier rules and constraints.

At the enterprise level, DoD’s federated EA is a set of architectures depicting slices of capability and function that provide guidance to decision-makers regarding:

- “What we must do”—A common set of principles, rules, constraints, and best practices that must be followed to meet enterprise goals
- “How we must operate”—The operational context of the aforementioned principles, rules, constraints, and best practices
- “When we will transition”—A roadmap (transition plan) with priorities, strategies for achieving them, and milestones, metrics, and resources needed to execute the strategies.

The DoD enterprise-level architectures do not provide implementation guidance or design details for individual systems or solutions, and are not a substitute for management decisions. They inform enterprise-wide decisions and portray the results. Transition planning adheres to the Department’s tiered accountability principle; it is done at the mission, business, and enterprise services layers of the target DoD EA.

This section provides information on the plan for modernizing and progressing the DoD EA to a future target state. Each MA and key Component will be addressed by describing goals and objectives for modernization and aligning initiatives, systems, services, and timelines for achieving the modernization goals and objectives.

### 4.1.1 Enterprise Information Environment Mission Area Modernization

Table 4 describes the planned modernization for the EIE MA. The DoD CIO recently published a 10-Point Plan for IT Modernization. This plan is the basis for the EIE MA modernization. The expected benefits of a successful EIE MA modernization are:

- Increased Mission Effectiveness
- Faster Capability Deliveries
- Strengthen Cyber Security
- Improve Interoperability
- Improve Outcomes of IT Acquisition
- Savings Through Cost Efficiencies.

<table>
<thead>
<tr>
<th>Goals</th>
<th>Objectives</th>
<th>Ways and Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consolidate Infrastructure</td>
<td>Consolidate Enterprise Networks</td>
<td>• Consolidate data centers and network operations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Optimize to a joint enterprise architecture with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>secure access</td>
</tr>
</tbody>
</table>

Table 4. Enterprise Information Environment Mission Areas Modernization
### Goals | Objectives | Ways and Means
---|---|---
Deliver DoD Enterprise Cloud | • Develop and execute a strategy and standards for a secure DoD cloud environment  
• Leverage commercial clouds that meet cybersecurity requirements |
Standardize IT Platforms | • Minimize program-unique platforms  
• Drive DoD use of standard platforms  
• Design platforms that ensure a secure cyber environment |
Enable Agile IT | • Lead the development of an Agile IT development methodology  
• Provide guidance to DoD on Agile IT best practices |
Streamline Processes | Strengthen IT Governance | • Restructure IT governance boards for enterprise view  
• Improve DoD IT decisions, strategies, and investments  
• Streamline compliance processes |
Strengthen Cybersecurity | • Implement an enterprise approach for the procurement of common IT H/W & S/W  
• Establish a DoD Commodity Council |
Leverage Strategic Sourcing for IT Commodities | • Develop enterprise cyber-situational awareness, including authentication  
• Leverage automated tools continual assessments  
• Streamline certification and reinforce reciprocity |
Strengthen IT Investments | • Obtain transparency of IT investments  
• Align IT investments to DoD strategies  
• Review performance of major investments |
Improve Enterprise Architecture Effectiveness | • Transition document-based process to decision support model  
• Develop EA Implementation Plan and Instruction |
Strengthen Workforce | Modernize IT Guidance and Training | • Provide guidance to DoD on adoption of Agile IT best practices  
• Leverage ongoing workforce initiatives  
• Develop a robust IT acquisition community |

### 4.1.2 Warfighting Mission Area Modernization
The content for this section will be available in future document releases.

### 4.1.3 Business Mission Area Modernization
The Deputy Chief Management Officer’s (DCMO’s) Enterprise Transition Plan (ETP) provides the context and perspective for understanding the Department’s transformation progress. The ETP incorporates the transition plans of the military services, Components, and the DoD.
enterprise. It provides a roadmap for achieving the DoD’s business transformation by implementing changes to technology, process, and governance, and identifying business investments that provide enterprise capabilities to support the warfighter and decision-makers. The ETP contains time-phased milestones, performance metrics, and a statement of resource needs for new and existing systems that are part of the BEA and Component architectures. It also includes a termination schedule for legacy systems that will be replaced by systems in the target environment.

The DCMO ETP includes: 1) the acquisition strategy for new systems that make up the target EA; 2) a list of business legacy systems not expected to be in the target environment; 3) a list of legacy systems expected to be part of the target environment; and 3) time-phased milestones, performance metrics, and a statement of resource needs. Updated annually, the DCMO ETP is an integrated product used with the Report on Defense Business Operations and the BEA to provide important information to DoD leaders to help them evaluate progress, gaps, and overlaps between current programs so they can redirect efforts to provide needed business capabilities.

4.1.4 Intelligence Mission Area Modernization

The content for this section will be available in future document releases.

4.1.5 Component Modernization

The content for this section will be available in future document releases.

4.2 Joint Information Environment (JIE)

In August 2010, the Secretary of Defense directed the consolidation of IT infrastructure to achieve savings in acquisition, sustainment, and manpower costs and to improve DoD’s ability to execute its missions while defending its networks against growing cyber threats. Specific direction was received to consolidate IT infrastructure to optimize for the joint environment and to pursue consolidation in a way that does not preclude future consolidation of IT infrastructure at the DoD enterprise level.

Consequently, this strategy focuses on requirements to: 1) Improve Mission Effectiveness, 2) Improve Cyber Security, and 3) Deliver Efficiencies. With sustainable and measureable progress in each of the areas above, the following enterprise outcomes can be achieved:

- Business systems have the necessary enterprise infrastructure services (including advanced cybersecurity, mobility, and cloud solutions) to support their system and processes without building separate infrastructure
- Secure mission-driven access to information and services is enabled across the enterprise
- The required Information Technology infrastructure is provided at lower cost through economies of scale, elimination of duplicative services and products, streamlined acquisition, and better use of industry best practices

A primary enabler of this strategy is the planned Joint Information Environment (JIE). Defense Business Systems (DBS) should leverage the JIE to provide shared information technology (IT) infrastructure with enterprise services and a single security architecture. As part of this:
There should be no DBS whose primary purpose is to provide “information technology and information assurance infrastructure” – all such infrastructure should be provided as “Enterprise IT infrastructure”.

While some defense business systems currently purchase or manage infrastructure dedicated to the individual business system, these systems migrate away from this stand-alone infrastructure at the earliest practicable opportunity (e.g., in conjunction with a technology refresh, or when a contract for commercial or mission partner IT infrastructure expires).

Where a defense business system has a unique requirement to use commercial or mission partner IT infrastructure (for example, where the required capability is best provided by commercial cloud computing services), these infrastructure connections must follow the appropriate Global Information Grid (GIG) connection approval, authorization, and waiver processes.

Implementation of this strategy is key to enabling cost-effective business systems.

4.2.1 Enterprise IT Infrastructure and Sub-functions

Enterprise IT Infrastructure consists of the shared information capabilities of the GIG that support systems, applications, and services that provide specific business, warfighting, or intelligence functions.

GIG. The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

The foundational concept for the future of Enterprise IT Infrastructure in the Joint Information Environment (JIE):

JIE is a secure Joint Information Environment, comprised of shared information technology (IT) infrastructure, enterprise services, and single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. JIE is operated and managed per Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs).

The Enterprise IT Infrastructure function consists of five sub function that the JIE aligns to. (also known as the JIE Big Rocks):

1. **Network Normalization:** Network normalization aligns the infrastructure to a joint common baseline and increases situational awareness, interoperability, and reduces the overall footprint of the Department. Key components include consolidating networks that do not align to our long-term strategy of a common DoD network under a common security framework. Key elements of this sub function are:
   - Standardizing the DoD Boundary with Internet;
   - Simplifying routing schema
   - Providing Security to the Enterprise Level – ending the practice of control points for every enclave
2. **Identity Management / Access Control:** Identity Management and Access Control moves the Department to a framework where users can access the network from anywhere on the globe and have access to information required to perform their duties and mission based upon their identity attributes. As a pilot program, the DoD CIO has directed implementation of the DoD Visitor Initiative which allows soldiers, sailors, airmen and marines as well as DoD employees to access their information that currently resides on Military Service-centric networks from any Post, Camp, Station, or Base while traveling. Key elements of this sub function are:
   - A Single authoritative source of User Identification/Authentication on any device in DoD (including mobile)
   - Access based on user attributes and roles (includes data tagging)

3. **Enterprise Data Center Consolidation:** The Department is capitalizing on the Federal Data Center Consolidation Initiative through a Service based approach; under JIE the Department will leverage these efforts and further consolidate. Accomplishing this objective will enable the department to achieve greater efficiencies, while enhancing data security, and increasing mission effectiveness. Key elements of this sub function are:
   - Core Data Centers based on standard Data Center architecture and enterprise implementation plan
   - DoD Component applications and data transition to Core Data Centers (Franchised Business Model)

4. **Enterprise Services:** Enterprise solutions will be regionally focused, and rapidly tailorable to support changing mission requirements. Over a ten year lifecycle, the potential to realize savings by replacing legacy equipment and moving to an almost everything over IP environment with Enterprise Services is significant. Key elements of this sub function are:
   - Federation of Enterprise Services approach
   - Global deployment of common services across Core Data Centers like:
     - DoD-wide Directory Service
     - ID and access management
     - Unified Communications capability
     - Messaging
     - Records Management
     - Portal and Collaboration
     - Enterprise Cross Domain Services
     - Enterprise file Storage
   - DoD Mandated Use of Mandatory and Shared Services (e.g. – like “Google search”, DoD white pages, etc.)

5. **Enterprise IT Governance:** The DoD governance structure is evolving to further support JIE Governance and continues to assure that all governance is aligned to the Department’s requirements, budgeting and acquisition processes. Oversight and guidance for JIE governance is provided by JIE Executive Committee (EXCOM). Day-to-day synchronization of JIE activities is performed by JIE Planning and Coordination Cell. DoD CIO continues to provide DoD IT governance lead. The operational sponsor is USSTRATCOM, delegated to USCYBERCOM. The technical and implementation lead is the JIE Technical Synchronization Office comprised of Defense Information Systems
Agency SMEs in concert with Service and Agency Representatives. Key elements of this sub function are:

– Senior DoD IT board focused on IT strategic planning, capital investment planning, cyber security, investment management, and systems acquisition, development and integration

– Streamlined current governance

– Collapsed and synchronized governance boards and forums

– Focused compliance enforcement to achieve the JIE end-state

4.2.2 Vision

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

- Secure access to information for the warfighter from any device
- Consolidated/standardized elements of networks to more effectively defend them and confront threats with agile information sharing
- Policies, procedures, oversight, and culture that enable info sharing

The vision for the JIE is shown in Figure 5, where the user has access at the point of need, regardless of where he/she is at, and what platform is used (home, thick, thin, slim, mobile, and future devices). The Tactical Edge is depicted by both the Disconnected/Intermittent/Low-bandwidth (DIL) detached and attached mode. As it is with Cloud computing, the tactical edge drivers are to fill the cloud efficiently, send data once, send only what is needed, and support DIL communications. The Detached Mode Cloud signifies those instances where warfighter encounters a situation where connectivity is broken (for whatever the reason); however, the warfighter is still able to operate based off of the data and capabilities that have been pushed or pulled prior to detachment. The Attached Mode Cloud depicts instances where LIMFACs for the warfighter include limited bandwidth, reduced/limited data storage, computing capabilities, and/or access to full-up applications. The Enterprise Information Environment (EIE) consists of the foundational computing infrastructure and both the common enterprise services and Service Mission applications which enable DoD users to discover, access, and use information to accomplish their missions. The “Applications” consists of a pool of capabilities (applications, widgets, etc.) that include common enterprise services as well as Service Mission applications from the Business, Warfighting, and Intelligence Mission Area applications residing on the computing resources and utilizing the data contained within the EIE. The “Data” consists of a pool of computing resources that provides secure, reliable, scalable, low-latency content storage and hosts a highly parallel analytic engine used to analyze and search authoritative, exposed, and secured data. The “Computing” consists of a pool of computing resources used to host services and applications.
Figure 5. Joint Information Environment End-State

Figure 6 provides a timeline for the major JIE increments. The model follows the efforts from Shaping to Sustainment. Each major increment has a set of identified Capabilities, the methods and maturity of the Operate and Defend domain, and the set of Governance concepts planned developed at each release increment.

<table>
<thead>
<tr>
<th>FY2012</th>
<th>FY2013</th>
<th>FY2014</th>
<th>FY2015</th>
<th>FY2016</th>
<th>FY2017</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHAPE</td>
<td>NORMALIZE</td>
<td>OPTIMIZE</td>
<td>SUSTAIN</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Capabilities:**
- Initial Enterprise Data Centers (5 more DCs)
- Initial Tactical Data Centers
- 50% E-Mail Portal
- DOD Record solution
- Data Engineer, IOC
- Cross Domain FOC
- Initial Unified Capabilities
- Current Security

**Operate & Defend**
- Big Rock SOP and TTPs implemented
- Integrated security hardening into JIE construct
- Governance

**Governance**
- Establish initial governance structure
- DTIM & FROCM
- Risk Assessment

**Capabilities:**
- Final phase of Enterprise Data Centers (10 more Data Centers)
- Final Tactical Data Centers
- Cloud E-Mail Contract
- Unified Capabilities
- Current Security
- Unified Capabilities
- Current Security

**Operate & Defend**
- Fully integrated and integrated Network Ops & Security
- Unified Capabilities
- Unified Capabilities
- Unified Capabilities

**Governance**
- Unified Capabilities
- Unified Capabilities
- Risk Assessment

**Capabilities:**
- Unified Capabilities
- Unified Capabilities
- Risk Assessment

**Operate & Defend**
- Unified Capabilities
- Unified Capabilities
- Risk Assessment

**Governance**
- Unified Capabilities
- Risk Assessment

**Governance**
- Unified Capabilities
- Risk Assessment

**Governance**
- Unified Capabilities
- Risk Assessment

**Governance**
- Unified Capabilities
- Risk Assessment

**Governance**
- Unified Capabilities
- Risk Assessment

Figure 6. Joint Information Environment Increment Planning
4.2.3 Alignment to the DIEA

The JIE aligns directly with the DIEA, as seen in Figure 7. The DIEA and the JIE will continue to support each other as the JIE progresses through incremental development. The DIEA will continue to provide high level guidance in the development of JIE IT solutions and the JIE will provide feedback so that the DIEA will evolve as an integral guidance and direction that support the strategy and guidance of the CIO.

Figure 7. Joint Information Environment Alignment with DIEA
5 Appendix 1: IT Asset Inventory

IT Asset Inventory provides a list of IT assets agency-wide to include all IT systems and services that support mission, administrative, and commodity IT programs, using the Federal Enterprise Architecture Reference Model taxonomies provided in the Common Approach. For the August 2012 Enterprise Roadmap submission, the IT Asset Inventory is optional.

In the Department of Defense IT Asset Inventory content is provided from asset information in the DoD Information Technology Portfolio Registry (DITPR). The DITPR provides an inventory of DoD IT Systems for assets inventory control and investment management.

Additional and improved IT Asset Inventory content for the DoD IT Asset inventory will be supplied in future document versions.

Today the DITPR serves as the repository for system information used to manage Component IT. It also meets a wide variety of internal and external compliance reporting requirements (e.g., Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Federal Information Security Management Act [FISMA] 2002, E-Authentication, Privacy Act, Privacy Impact Assessments, and Interoperability).

Plans are to integrate DITPR with the IT Budget (SNaP-IT) and the Enterprise Mission Assurance Support System (eMASS) to support IT investment management and manage the DoD IT portfolio. The upgrade of DITPR will improve IT Budget and IT Systems Inventory (SNAP-IT and DITPR) integration and data reconciliation. It will implement periodic system changes to accommodate new Congressional and OMB reporting requirements for the IT Asset Inventory, IT Budget, and IT Portfolio Management and it enables the ability to conduct quality assurance for DoD IT Portfolio Repository (DITPR) data. The result will be increased ability to provide authoritative and accurate information about IT systems and investments in DoD. DoD will achieve improved decision-making about IT investments; information to enable proactive cost-estimation for IT initiatives; better visibility over Joint Information Environment implementation status; support for DCMO Investment Review Board (IRB) process.

DoD Information Technology Portfolio Repository (DITPR)  
https://ditpr.dod.mil/
6 Appendix 2: Commodity IT Consolidation Plan

6.1 Agency COO Communication to the Agency

In 2010, Secretary Gates initiated renewed efforts\(^5\) to realize Information Technology efficiencies, eliminate duplicative services and products, share technologies across the Department, adopt agile practices, and enterprise business strategies, and adopt industry best practices.

The DoD is an immense and complex organization. It has more than 1.4 million men and women serving on active duty, employs 750,000 civilian personnel, and 1.1 million National Guard and Reserve personnel, making it the nation’s largest employer. In addition, more than 5.5 million family members and military retirees receive benefits as a result of their past service or their relationship to a service member.

The DoD organization includes the Office of the Secretary of Defense, the three Military Departments (Department of the Army, Department of the Navy and the Department of the Air Force), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the nine Combatant Commands, the Office of the Inspector General of the Department of Defense (IG DoD), and numerous Defense Agencies and DoD Field Activities.\(^6\)


On March 30, 2012, the White House Office of Management and Budget (OMB) issued Memorandum M-12-10, Implementing PortfolioStat.\(^7\) The memo included several directives. One directive was for DoD’s COO to designate a lead for the PortfolioStat Initiative responsible for implementing the PortfolioStat process and guidance and inform OMB of the designation. DoD responded, appointing the DoD CIO as the lead.

OMB Memorandum M-12-10 also called for agencies to provide a formal communication to the agency summarizing the specific actions to be taken to comply with the guidance. On May 29, 2012, the DoD CIO issued a memorandum, “Data Call for Implementing PortfolioStat,” providing direction to Components for meeting OMB’s requirements for Commodity IT baseline data and for CIO Commodity IT Consolidation Plans.

---


\(^3\) U.S. Department of Defense Organization Chart, [http://www.defense.gov/organizationchart/38](http://www.defense.gov/organizationchart/38)

\(^4\) White House Office of Management and Budget Memorandum M-12-10, Implementing PortfolioStat, March 30, 2012, [http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-10_1.pdf](http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-10_1.pdf)
Given the Department’s size and diverse mission needs, this consolidation will require significant effort. Nevertheless, it is imperative that we rise to this challenge, since these efforts will make the Department’s IT Infrastructure more effective and secure, while providing efficiencies that continue our stewardship of American taxpayers’ dollars.
6.2 Executive Summary

In August 2010, Secretary Gates announced the Department’s Efficiencies Initiative.8 In December 2010, then-Federal CIO Vivek Kundra released the 25-Point Implementation Plan to Reform Federal Information Technology Management9 These two efforts spurred subsequent documents providing guidance for implementation. This guidance includes the DoD Information Technology Enterprise Strategy and Roadmap (ITESR)10; the Defense Business Board’s Linking and Streamlining the Defense Requirements, Acquisition and Budget Processes report11; and DoD CIO’s 10-Point Plan for IT Modernization.12 Major areas of effort focus around data center consolidation, cloud computing, a strategy for shared services, commodity IT, and digital government.

DoD’s overall strategy surrounding this effort is to centralize visibility and oversight with decentralized execution by Components. Goal 3 of the DoD Information Enterprise Strategic

“...There are great benefits to be gained – in cost, and efficiency – from taking advantage of economies of scale. The problem is that too many parts of the department, especially in the information technology arena, cling to separate infrastructure, and processes. All of our bases, operational headquarters, and defense agencies have their own “IT” infrastructures, processes, and application-ware. This decentralization approach results in large cumulative costs, and a patchwork of capabilities that create cyber vulnerabilities, and limit our ability to capitalize on the promise of information technology. Therefore, I am directing an effort to consolidate these assets to take advantage of the Department’s significant economies of scale, thereby creating savings in acquisition, sustainment, and manpower costs.”

- Secretary of Defense Robert M. Gates

---


Plan 2010-2012 calls for “Synchronized and Responsive Operations,” and elaborates on this vision: “The DoD Information Enterprise infrastructure, critical assets, and capabilities are operated, secured, and defended in a synchronized manner by all DoD Components to support commanders in achieving mission success.”\textsuperscript{13} The document further calls to “Improve the alignment of organizational responsibilities and reporting channels to provide centralized management oversight of compliance/enforcement of all operational aspects of the DoD IE.”\textsuperscript{14}

These ongoing efforts are being undertaken across the Department, led by the Component CIOs who manage and provide most of DoD's IT infrastructure: DoD CIO and the CIOs of the Office of the Secretary of Defense, Departments of the Army, Navy, and Air Force; Defense Information Systems Agency (DISA); Defense Logistics Agency (DLA); the Defense Finance and Accounting Service (DFAS); and U.S. Transportation Command (TRANSCOM). Major initiatives include data center consolidation, moving to a cyber-secure cloud environment, the use of shared services, and rationalization of defense business systems, and IT infrastructure and services. This concentration of effort will have a cumulatively beneficial impact.

6.3 Scope and Complexity

The DoD is an immense and complex organization. It has more than 1.4 million men and women serving on active duty, employs 750,000 civilian personnel, and 1.1 million National Guard and Reserve personnel, making it the nation’s largest employer. In addition, more than 5.5 million family members and military retirees receive benefits as a result of their past service or their relationship to a service member.

The DoD organization includes the Office of the Secretary of Defense, the three Military Departments (Department of the Army, Department of the Navy and the Department of the Air Force), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the nine Combatant Commands, the Office of the Inspector General of the Department of Defense (IG DoD), and numerous Defense Agencies and DoD Field Activities.15

Geographically, DoD supports personnel in more than 146 countries, at over 6,000 locations, in more than 600,000 buildings and structures.

DoD supports more than 10,000 operational systems, 20 percent of which are mission critical. DoD utilizes more than 700 data centers, 67,000 servers, more than 7 million computers and IT devices, and thousands of networks. DoD’s tally to support a mobile workforce includes 250,000 Blackberries, 5,000 iOS systems, and 3,000 Android systems.

Information advantage is a critical element of national power. It requires the effort of the entire DoD to provide an information environment optimized for the warfighter that is effective for all echelons, from the tactical edge to the strategic core. The complexity of the organization has contributed to building an IT system of unnecessary complexity and redundancy. DoD efforts to modernize IT look to consolidate the infrastructure, streamline processes, and strengthen the workforce.

The DoD and its mission partners increasingly demand rapid delivery of secure information capabilities. Stove-piped IT systems, hundreds of sub-optimal data centers and networks, limited interoperability, and slow IT delivery hinder the Department from meeting this demand. To meet these needs, DoD is targeting redundancy, inefficiency, and duplication of effort to create a more streamlined, efficient, and agile IT environment.

6.4 DoD Areas of Focus

The DoD CIO; the CIOs of the Departments of the Army, Navy, and Air Force; and all other DoD Components (especially those with large IT budgets such as the Defense Information Systems Agency (DISA), Defense Logistics Agency (DLA); the Defense Finance and Accounting Service (DFAS), and U.S. Transportation Command (USTRANSCOM)), are working diligently to reduce redundancy, maximize efficiency, and create agility. Through data center consolidation, cloud computing solutions, shared services, network consolidation, strategic sourcing, a mobile device strategy, and the Campaign to Cut Waste through IT Efficiencies, DoD is effecting changes that will result in savings, efficiencies, and modernizing IT across the Department. The end result will be the availability of better aligned products and

---

services for warfighters, business, and intelligence missions. Below are highlights of DoD ongoing efforts.

6.4.1 Data Center Consolidation

The Information Technology Enterprise Strategy and Roadmap (ITESR) Initial Implementation Plan (IIP) names data center and server consolidation as one of eight initial initiatives to target in order to meet the Secretary’s direction to realize efficiencies. The goal outlined is to optimize DoD computing centers and establish core computing centers to support critical enterprise services.\(^\text{16}\)

DoD and its Components are considering all options for achieving consolidation. These include migrating infrastructure to Defense Information Systems Agency (DISA) enterprise computing centers (DECCs), valid commercial options to reduce costs of IT services, cross-Component co-hosting, and virtualization/cloud computing, to name a few. The Air Force, Army, and the Defense Logistics Agency (DLA) have adopted a “DISA First” strategy for data center consolidation. With the “DISA First” strategy, they will consider DISA for application and data hosting before pursuing other solution centers.\(^\text{17}\) DoD’s approach for consolidation consists of increasing reliance on core data centers to support critical enterprise services and reduce Component data centers. The core data centers will gradually absorb many of the applications and services currently hosted in numerous Component data centers, enabling the latter to be closed.\(^\text{18}\) Core data centers will deliver both newer cloud-based services as well as legacy services. The Data Center Consolidation Plan calls for the reduction of 772 data centers open in FY10 to 532 by FY13, and to 480 by FY14. DoD closed 57 data centers in FY11.

DoD is developing the DoD Data Center and Server Consolidation Reference Architecture. This DoD-wide reference architecture is intended to guide enterprise and DoD Component efforts for consolidating and optimizing data centers to achieve Department goals as part of the ITESR.\(^\text{19}\)

DoD Component Data Center Consolidation Plans

DoD Components are developing consolidation plans to reduce their data center inventory. Examples of Components’ consolidation efforts are provided below.

**Army:** The Army will use the Application Migration Concept of Operations as a guide to consolidate and migrate applications from its current local and functional data centers to DoD enterprise data centers. In addition, a memorandum issued by the Secretary of the Army on September 9, 2011, directs that the Army's 2010 moratorium on the procurement of all servers will be expanded to include a moratorium on the construction and/or renovation of Army data centers and server rooms. In particular, the memorandum prohibits the procurement of servers and the construction or renovation of hosting facilities without a written waiver granted in advance by the Headquarters, Department of the Army (HQDA), CIO/G-6, consistent with the HQDA Army Data Center Consolidation Plan Execution Order published on May 9, 2011.

\(^{16}\)Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap Initial Implementation Plan, Version 1.0, November 4, 2011, p. ii.


Navy: By March 2012, the U.S. Navy had closed 13 data centers and plans to close approximately 23 more during the next fiscal year. Additionally, during the past five years, the Space and Naval Warfare Systems Command (SPAWAR) has transitioned a number of applications out of existing data centers and into SPAWAR hosting facilities. “Consolidating more than 150 data centers into fewer, more modern, standardized and efficient enterprise data centers will enhance network security and reduce complexity.”

Marine Corps: The Marine Corps is evaluating local computing centers and isolated server hosting facilities for opportunities to consolidate. The Marine Corps plans to complete regionalization of IT infrastructure assets into its four enterprise and seven regional data centers. The Marine Corps Enterprise IT Services Center in Kansas City, Mo., has opened and will be the centerpiece of the Marine Corps data center consolidation strategy.

Air Force: The Air Force is undertaking the Air Force Network Migration. A major objective of the program is to collapse the multiple Air Force Major Command (MAJCOM) Active Directory (AD) and Microsoft Exchange architectures into a single, consolidated, centrally-managed Air Force enterprise architecture. This provides decision makers with unmatched situational awareness, and command and control of network forces.

The Air Force is also working to consolidate its network IT. This effort seeks to reduce the number of Air Force servers through virtualization, and will consolidate nine MAJCOM, and regional processing centers into five centralized enterprise area processing centers. This initiative will prepare the Air Force for further consolidation into enterprise computing facilities as recommended by DISA.

Air National Guard (ANG): The Air National Guard Network Control Center Rebuild initiative is deploying a consolidated and standardized virtual infrastructure platform to all of the ANG data centers. This will result in significant reduction in physical server counts, floor space, cooling requirements, and power costs. The ANG plans to reduce 48 more data centers through this initiative in FY12.

Additional Consolidation Candidates: The Air Force MAJCOMs, excluding the ANG, identified a total of 32 data centers that could be closed between FY12 and FY15.

Defense Logistics Agency (DLA): The DLA approach consists of several elements:

- Virtualize existing applications
- Migrate applications to DISA Defense Enterprise Computing Centers (DECCs)
- Consolidate DLA test and development environments
- Establish application development standards

Military Health System (MHS): MHS is considering the following options as part of its efforts to reduce infrastructure: decommissioning, site centralization, server/storage virtualization,

---


virtualization, and cloud computing. MHS’ implementation plans seek to achieve a reduction of 50 percent or more (the target is 70 percent) of its data centers.

**Defense Commissary Agency (DeCA):** DeCA’s approach to the virtualization effort is multifaceted. It includes virtualization of the current operating environment and upgrading and streamlining current systems to accommodate the more technologically advanced virtual environment. DeCA wants to reduce its energy consumption footprint and reduce server management, contract support, and provisioning through improved automation. This goal requires complete system refreshes in some instances and code modifications in others.

### 6.4.2 Cloud Computing

Many DoD Components are migrating systems and data storage to cloud solutions. Below are examples of current cloud solution activities being undertaken across entire Department, and within the Army, Navy, and Air Force.

**Army:** Using DISA as a service provider, the Department of Defense is offering Components an enterprise email service. DISA will manage and provide full lifecycle service for computing, storage, and network infrastructure using Microsoft Exchange 2010 and nine Defense Enterprise Computing Centers. Initial customer base is 1.4 million unclassified users and more than 200,000 classified users. Defense Enterprise Email (DEE) was initiated with Army as the first Component to migrate. The Army is expected to complete the phased transition to Enterprise Email within the 18 month window. Other Components migrating to DEE include US Transportation Command, US African Command, and US European Command.

**Air Force:** The Air Force Personnel Center (AFPC) moved and upgraded its Customer Relationship Manager (CRM) tool from one hosting environment to DISA’s private cloud. Air Force members (active, guard, reserve, retirees, and civilians) are seeing increased availability because they can now access personnel services and applications 24/7 from any domain. In the past, Air Force members were only able to access these services from a .mil domain. DISA’s cloud environment also offers redundancy, allowing increased performance for Air Force members. Transactional data is synchronously replicated into DISA’s alternate site. In case of a disaster, operations are shifted to the alternate site.

### 6.4.3 Shared Services

On May 2, 2012, OMB published the Federal Information Technology Shared Services Strategy. The document is a follow-up to the 25 Point Implementation Plan to Reform Federal Information Technology Management. Both documents seek to increase return on investment, eliminate waste and duplication, and improve the effectiveness of IT solutions. Commonly referred to as “Shared-First,” this strategy requires agencies to use a shared approach to IT service delivery. It defines shared service as “a function that is provided for consumption by multiple organizations within or between Federal Agencies.”

DoD has many ongoing shared service initiatives taking place that meet the OMB shared service definition of a “a function that is provided for consumption by multiple organizations.” Later in

---


24Executive Office of the President Federal Information Technology Shared Services Strategy, May 2, 2012, p. 17, [http://www.whitehouse.gov/blog/2012/05/02/introducing-it-shared-services-strategy](http://www.whitehouse.gov/blog/2012/05/02/introducing-it-shared-services-strategy)
this document, we highlight two DoD shared service initiatives: The Unclassified Information Sharing Service/All Partner Access Network (UISS/APAN) and the General Fund Enterprise Business System (GFEBS).

6.4.4 Other Efforts

In addition to the areas covered above, DoD and its Components have been working across a number of initiatives to consolidate IT. Many of these efforts, introduced in the DoD CIO’s 10-Point Plan for IT Modernization, the Mobility Strategy, and the Campaign to Cut Waste, are reviewed below.

**Network Consolidation**

**Background and Overarching Principles:** As part of the DoD CIO’s 10-Point Plan for IT Modernization, DoD has undertaken steps to consolidate enterprise networks. The goal is twofold: to consolidate data centers and network operations and to optimize to joint enterprise architecture with secure access.

**Approach:** Consolidating data centers and network operations entails:

- Development and implementation of enterprise-level guidance, policies for IT optimization and consolidation; and
- Achieving further consolidation by integrating and capitalizing on test and integration centers.

Optimizing to joint enterprise architecture involves:

- Using centrally managed architectures that use standardized joint processes; and
- Defining common security architecture of core and DoD network infrastructures.

These efforts are ongoing.

**Mobility Device Strategy**

**Background and Overarching Principles:** The envisioned end state outlined in ITESR is that “users will have timely access to the information and resources they require, anywhere and anytime across the DoD Information Enterprise, enabling them to make informed decision in executing their missions.” Mobile devices play an important role to accomplish this vision.

Further, ITESR lays out end-user services focused on improving mission effectiveness and reducing costs by taking advantage of rapid changes and advances in the type of devices used to access information and applications, as well as changes in the operating systems on which those systems are built. DoD CIO’s mobility vision is similar: “a highly mobile workforce equipped with secure access to information and computing power anywhere, at any time, for greater mission effectiveness.” DoD CIO has outlined the following goals for mobile communications:

- Advance and evolve the DoD Information Enterprise infrastructure to support mobile devices;

---

27 Department of Defense Mobile Device Strategy, Version 2.0, April 2012, p. 4
Evolve spectrum management;
Expand infrastructure to support wireless capabilities;
Establish a mobile device security architecture;
Develop mobile device policies and standards;
Institute mobile device policies and standards;
Establish a mobile device management service;
Educate and train mobile device users;
Promote the development, and use of DoD mobile and web-enabled applications;
Establish a common mobile application development framework;
Institute a mobile application certification process;
Provide an enterprise mobile application environment; and
Web-enable IT capabilities for mobile device support.\(^{28}\)

**Approach:** On April 6, 2011, the Use of Commercial Mobile Devices memorandum\(^{29}\) provided guidance, and a way for DoD Commands to employ new technologies and tests. The memorandum also established the Commercial Mobile Device Working Group, with representation from the Services, to assess progress.

On May 14, 2012, the DoD CIO issued a memorandum calling for an alignment of the progress of various mobile device pilots and initiatives across DoD under common objectives, ensuring that the warfighter benefits from these initiatives. It also calls for these efforts to align with efforts composing the Joint Information Environment (JIE). The DoD CIO describes JIE goals and efforts as follows: “Our primary goals are to make the Department more effective and more secure against cyber threats and vulnerabilities. A secondary, but very important goal is to reduce the cost associated with the Department’s overall information technology infrastructure by simplifying, standardizing, centralizing, and automating infrastructure at the enterprise level. We are calling the result of the effort the Joint Information Environment, or JIE. We are using the intelligence community’s information technology modernization efforts to inform much of the JIE planning. A team consisting of experts from throughout DoD is currently fleshing out the approach and is developing an implementation plan of action and milestones, and cost estimates.”\(^{30}\)


**Strengthen IT Investments**

---

\(^{28}\)Department of Defense Mobile Device Strategy, Version 2.0, April 2012, p. 4
\(^{29}\)DoD CIO memorandum, Use of Commercial Mobile Devices (CMD) in the Department of Defense (DoD), [https://dodcio.osd.mil/SignedMemos/2011%20Archived%20Memos/Forms/AllItems.aspx](https://dodcio.osd.mil/SignedMemos/2011%20Archived%20Memos/Forms/AllItems.aspx)
Background and Overarching Principles: As part of the DoD CIO’s 10-Point Plan for IT Modernization, DoD has undertaken steps to strengthen IT investments. Consistent with the OMB M-12-10 requirement to "illustrate how investments within the IT portfolio align with the agency's mission and business functions," the goal is to establish a comprehensive IT Investment Management program to improve the transparency and management of the full portfolio of DoD IT investments.

Approach: Develop a comprehensive IT Investment Management program to strengthen existing procedures. The program will focus on examining the full DoD IT investment portfolio to optimize resources and capabilities needed to execute the DoD mission. A systematic plan and set of processes will be implemented to systematically review the full DoD IT Budget annually. This will include establishing reviews of major IT investments (not in formal acquisition programs) for system performance, funding execution, and enterprise alignment. Component CIOs will play an active role in these reviews and will conduct similar reviews at their level. Consistent with the OMB M-12-10 requirements, this approach would "Establish criteria for identifying wasteful, "low-value," or duplicative investments" and "Establish a process to identify these potential investments and a schedule for eliminating them from the portfolio."

Campaign to Cut Waste IT Efficiencies

Background and Overarching Principles: In accordance with the November 9, 2011, President’s Executive Order 35189 Promoting Efficient Spending, the Deputy Secretary of Defense issued a plan for implementing the executive order on December 29, 2011. On February 17, 2012, in her memorandum, Optimizing Use of Employee Information Technology Devices and Other Information Technologies to Achieve Efficiencies, the DoD CIO provided additional guidance.

That memorandum calls on the Department to identify opportunities to implement Department-wide IT solutions that consolidate activities such as desktop services, email, and collaboration tools; eliminate waste resulting from underutilized equipment, installed software, or services; and establish controls to ensure responsible stewardship. It defines employee IT devices as mobile phones, smart phones, desktop and laptop computers, and tablet personal computers.

The memorandum further calls for each DoD Component to:

- Provide guidance to limit the number of employee IT devices issued to employees to only those required to meet mission needs;
- Implement controls to ensure the Department is not paying for unused or underutilized equipment, installed software, or services;
- Provide the DoD CIO a plan by February 27, 2012, that includes a narrative of initiatives taken or intended to support the reduction; and
- Provide the DoD CIO the FY10 baseline expenditures for Employee IT devices no later than June 30, 2012.

On May 11, 2012, the DoD CIO issued an update, asking each Component to provide FY12 second quarter reporting by June 1, 2012, and to report their FY10 baseline expenditures and anticipated FY13 savings for employee IT devices and software by June 30, 2012. These efforts are ongoing.
**Strategic Sourcing**

**Background and Overarching Principles:** In accordance with the ITESR and as part of the DoD CIO’s 10-Point Plan for IT Modernization, DoD is working to consolidate the acquisition of enterprise software and commodity IT hardware. The goal is to reduce lifecycle costs for these items and to enhance secure access/interoperability.

**Approach:** Leverage in-place organizations, expertise, and exemplar DoD contracts

- Empower already identified teams and partner with USD AT&L on governance.
- Ratify previously identified commercial software and IT hardware items targets; and exemplar contract vehicles.
- Issue DoD CIO guidance with specific timetable and assignment of Component responsibilities.

### 6.5 IT Portfolio Management Overview

#### 6.5.1 Strengthening IT Governance

DoD CIO is collaborating with OSD partners to implement reforms that improve DoD decisions on IT strategies, investments, requirements, and acquisitions by leveraging enterprise architectures, analytic tools, and broad stakeholder collaboration. One initiative of the DoD CIO’s 10-Point Plan for IT Modernization is to strengthen IT governance.

**Background:** OMB Director Jacob Lew issued [memo M-11-29](http://m.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-29.pdf) on August 8, 2011, reinforcing CIO authorities as part of the 25 Point Implementation Plan to reform Federal IT management. The memo includes: “CIOs must work with Chief Financial Officers and Chief Acquisition Officers to ensure IT portfolio analysis is an integral part of the yearly budget process for an agency.”

[GAO Report 11-634](http://www.gao.gov/new.items/d11634.pdf) on Federal CIOs outlined the 13 areas of responsibility CIOs have in the area of IT Management and Information Management as defined by law. These CIO responsibilities include IT strategic planning, capital planning and investment management, and systems acquisition, development, and integration. The GAO reinforced the importance of fully implementing these CIO responsibilities within each federal agency.

**Approach:** The DoD CIO is undertaking a thorough analysis of current governance boards and of the ways in which the CIO community interacts with DoD strategic, PPBE, Joint Capabilities Integration and Development System (JCIDS), and acquisition processes. This analysis includes external participants to minimize the bias inherent in self-assessments. It will examine purpose, membership (depth and breadth), roles and responsibilities, processes, products, policies, and influence of the existing governing bodies. The analysis will evaluate how well each of the current governance bodies meets its stated purpose and will explore gaps in processes for achieving DoD CIO priorities. It will also examine statute, policies, initiatives, and recommendations from OMB, US CIO, SECDEF, and the Defense Business Board.

---


This analysis will drive a series of recommended improvements to the DoD IT governance structure, policies, and processes to be implemented over the next 12–18 months. The objective is simplified and streamlined governance procedures that leverage the existing Departmental processes. Once the improved procedures are in place, all IT governance boards must develop new charters detailing purpose, membership, roles and responsibilities, processes, and products for approval within three to six months. Any IT governance board that does not have a new charter approved in six months will be disbanded until one is approved.

The overall intent of improving these governance structures is to enable Agile IT practices and provide an enterprise approach to investment and development strategies.

Lastly, the DoD CIO will eliminate the need for IT programs to develop and submit separate CCA compliance documentation. CIOs (or designee) shall confirm CCA compliance by participating in milestone meetings. Clinger Cohen Act requirements will be analyzed against existing acquisition and related documentation. Any CCA requirement not already included in the documentation that is collected in accordance with the Department’s acquisition process (DoDI 5000.02 which is jointly signed by the Under Secretary of Defense for Acquisition, Technology and Logistics and the DoD CIO) will be managed via CIO processes.

### Strengthening IT Governance Schedule from 10 Point Plan to Modernize Department of Defense Information Technology

<table>
<thead>
<tr>
<th>Task Description</th>
<th>3QFY12</th>
<th>4QFY12</th>
<th>1QFY13</th>
<th>2QFY13</th>
<th>3QFY13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct analysis on CIO interaction with major DoD processes, current governance boards, and management tools.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis of CCA documents and processes mapped to Acquisition model</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Draft CCA DTM, collaborate with Service CIOs/SAEs, and sign DTM</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide recommendations on DoD IT governance structure, policies, and processes.</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coordinate and implement new governance processes and any new governance forums</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

---

6.5.2 Program Management

The DoD CIO serves as the IT Functional Leader (FL) for the IT acquisition workforce, part of the Defense-wide acquisition workforce. In that role, the DoD CIO oversees the education, experience, and training requirements for the IT acquisition workforce and serves as the senior DoD subject matter expert for IT acquisition training requirements. The DoD CIO as IT FL also serves on the Senior Steering Board, the highest level governing board for acquisition workforce training. The DoD CIO also chairs the IT Functional Integrated Process Team (FIPT), which provides broad representation from the DoD Services and Agencies.

Each acquisition career field, including IT acquisition and Program Management (which encompasses IT program managers) has a specific set of progressive requirements for persons in that field at each of three levels: 1) journeyman; 2) mid-level; and 3) senior level. To be certified at each level, a person needs to meet an established set of education, training, and experience requirements. The certification standards for each field can be found at the following web address:  http://www.dau.mil/Training/default.aspx.

All acquisition program managers are provided training and are certified in accordance with the Defense Acquisition Workforce Improvement Act (DAWIA). The majority of formal training for acquisition program managers is provided by the Defense Acquisition University and the Information Resources Management College (iCollege).

In accordance with the Defense Acquisition Workforce Improvement Act (DAWIA), signed into law in November, 1990, each Service has a Service Acquisition Executive (SAE). Reporting to the SAE is the Defense Acquisition Career Management (DACM) office. Each Service and Agency DACM sets forth the annual performance plans and evaluation requirements for each person within their respective acquisition workforce.

The AT&L Workforce Education, Training, and Career Development Program implements DoD AT&L Workforce requirements established by Congress in Title 10, United States Code, Chapter 87. It supports the DoD Components by uniformly establishing the structure, policies, and procedures to enable the AT&L Workforce to achieve and maintain competencies required to serve successfully in AT&L positions. The AT&L Workforce Education, Training, and Career Development Program operates under a philosophy of centralized DoD policies and guidance, and decentralized execution by the DoD Components. Under DAWIA, the processes to monitor and improve performance of IT (and IT PMs) are done through the Components and USD (AT&L); the Functional Leaders, including the DoD CIO as IT FL, set the education and training standards and ensure that the training provided is in accordance with the established standards.

The Defense Acquisition Workforce Strategic Plan (2010)\textsuperscript{34} describes a series of initiatives to expand the capabilities of the acquisition workforce. Part of the strategic plan has been to grow key career fields, including the IT and Program Management career fields.

In addition, the USD(AT&L) and the DoD CIO signed the IT Acquisition Workforce Strategic Plan in April 2012. As part of this plan, the DoD CIO as IT Acquisition FL has outlined additional initiatives to further enhance the IT acquisition workforce, including a comprehensive IT acquisition workforce competency review.

\textsuperscript{34}Department of Defense (DoD) Fiscal Year (FY) 2010–2018 Strategic Workforce Plan \url{https://www.apps.cpms.osd.mil/shcp/FY-2010-2018%20SWP.pdf}
6.5.3 Information Security

DoD Directive 5144.135, signed May 2, 2005, addresses consolidation of IT security activities under the DoD CIO. Specifically, section 3.3.3 of the Directive states that the DoD CIO “Serve as the information architect for the DoD enterprise information environment, and provide oversight and policy guidance to ensure compliance with standards for developing, maintaining, and implementing sound integrated and interoperable architectures across the Department, including intelligence systems and architectures. Ensure that IA is integrated into architectures pursuant to section 3534 of reference (b) and section 11315 of reference (c).” Section 3.3.4 of the Directive states that the DoD CIO “Perform the duties and fulfill the responsibilities associated with information security and other matters under section 3544 of (sic) Title 44 of US Code.”

Section 3544 calls for the head of each agency to be responsible for “providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of information.”

In accordance with that responsibility, the DoD CIO outlined a Strengthen Cybersecurity objective as one of the 10 points contained in the DoD CIO’s 10-Point Plan for IT Modernization. According to the plan, “As part of this initiative, the DoD CIO will work with U.S. Cyber Command and the DoD Components to identify new capabilities and processes necessary to develop an effective cyber situational awareness capability consisting of automated data sharing, reporting, and thresholds for action. This situational awareness capability shall be documented as part of the IT infrastructure modernizations, included in the Computer Network Defense (CND) Architecture, and implemented as a near term priority in conjunction with the DoD’s efforts to consolidate IT resources and mature cloud solutions. Continuous monitoring of operational systems using automated tools will enable situational awareness for agile responses to threats. Well-designed and integrated automated tools will also support DoD systems and networks security operations and maintenance functions by enabling automated security assessment and continual security authorizations.”

DoD CIO also has several partnership initiatives designed to strengthen information security. The information capability delivery partnership with the DoD Components (in particular, DISA, NSA, USCYBERCOM, and the Military Department CIOs), other Office of the Secretary of Defense staff elements, as well as the Joint Chiefs of Staff. These organizations work together across all information capabilities and management functions to leverage the three major decision processes of the Department (requirements, budget, and acquisition) to determine the capabilities needed; plan and budget the necessary resources; acquire them in the most cost-effective and efficient manner possible; and ensure they are delivered in a trusted secure way. This partnership also integrates the policies and processes by which the Department generates, shares, protects, and defends information assets that drive their functions across the DoD.

---

38 DoD CIO 10 Point Plan to Modernize Department of Defense Information Technology, March 12, 2012, p. 12, see links under Strategy/Plans at https://dodcio.osd.mil/default.aspx#
39 Department of Defense (DoD) Chief Information Officer (CIO) Campaign Plan Summary, p. 6.
DoD CIO also has a secure information sharing partnership with mission partners, to include the intelligence community, industry, academia, international, federal, state, local, and tribal entities, as well as coalition nations and forces. This partnership works to achieve cross-organizational information sharing, while securing sensitive information and addressing threats and vulnerabilities to global infrastructure.  

6.6 Commodity IT Consolidation Plan

6.6.1 Enterprise Architecture

DoD has taken a federated approach for developing and managing the DoD Enterprise Architecture (EA) that is based on enterprise-level guidance, capability areas, and component architectures. A Federated DoD EA is the best way to effectively describe a complex Department and provide the necessary context and guidance to govern, manage, and accomplish the missions of the Department. This approach is described in a Federation Strategy that is currently being updated. The strategy describes an approach to enterprise architecture that facilitates interoperability and information sharing between semi-autonomous departments, components and programs. This approach recognizes the need for autonomy but requires linkages and alignment of architectures from the Program level up to the Enterprise level. A governance body and associated processes are in place to provide the necessary governance and oversight with respect to the strategy. The Governance body consists of subordinate working groups that contain Department-wide representation. Requirements for DoD EA compliance are captured in the CIO approved DoD Information Enterprise Architecture (IEA) document that is posted on the CIO public site for department-wide use.

DoD has instituted a policy requiring the registration of architectures in a DoD architecture registry system (DARS) that provides visibility and accessibility for all registered architectures. Other architecture requirements are imbedded in various policies in the Department such as the DoDD/I 4630, DoDD 8000, CJCSI/M 3170, and CJCSI 6212. Together, these policies provide the direction needed to maximize the sharing and use of architectures in key DoD processes. DoD has designated eighteen segments to guide and support IT investments and solutions in adherence with OMB guidance. The DoD EA is applied to guide investment portfolio strategies and decisions; define capability and interoperability requirements; establish and enforce standards; guide security and information assurance requirements across DoD; and provide a sound basis for transitioning from the existing environment to the future.

---

40Department of Defense (DoD) Chief Information Officer (CIO) Campaign Plan Summary, p. 6.
One of the 10 initiatives outlined in the DoD CIO’s 10 Point Plan to Modernize Department of Defense Information Technology is to improve enterprise architecture effectiveness.\textsuperscript{44} This effort will examine documented DoD strategies, mandates, and guidance, and conduct a stakeholder analysis to identify the key drivers to achieve mission outcomes. The DoD CIO will develop a new enterprise architecture program management plan that describes the vision, outcomes, strategy, governance, processes, and products for the DoD CIO enterprise architecture efforts. This program management plan will emphasize the need for improved interoperability across missions and infrastructure by implementing an IT infrastructure that is integrated, scalable, adaptable, and secure. The new IT infrastructure will facilitate agile development by supporting rapid component development and integration.

DoD will promulgate a DoD instruction that describes how the enterprise architecture will be used to realize outcomes and support DoD processes. The DoD CIO will designate a DoD IT Infrastructure architect to work with the DoD Chief Architect. The DoD IT Enterprise Architecture, currently in revision, will be reconciled with the ITESR and its associated implementation plan to better support IT modernization. Specific details of the new enterprise architecture and associated processes will be described in the enterprise architecture program management plan.

**Improve Enterprise Architecture Effectiveness Schedule from 10 Point Plan to Modernize Department of Defense Information Technology\textsuperscript{45}:**

<table>
<thead>
<tr>
<th>Task</th>
<th>3QFY12</th>
<th>4QFY12</th>
<th>1QFY13</th>
<th>2QFY13</th>
<th>3QFY13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop Enterprise Architecture Program Management Plan</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designate IT Infrastructure Architect</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Architecting Instruction</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Publish a DoD Enterprise IT Infrastructure Architecture</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Publish a DoD Enterprise Architecture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

**6.6.2 Agency Valuation Model**

In response to OMB Circular A-131, DoD produced the FY 2012 Value Engineering Program Management Plan, available through a link at [http://rtoc.ida.org/ve/ve.html](http://rtoc.ida.org/ve/ve.html). The Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) will soon release DoD Instruction 4245.nn, currently in draft form.


DoD’s valuation engineering process for IT investments has been integrated into the acquisition process and is explained in Chapter 7 of the Defense Acquisition Guidebook

6.6.3 Agency Criteria for Identifying Low Value Investments

The 2005 National Defense Authorization Act (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 DBSMC 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 National Defense Authorization Act for Fiscal Year 2010, which required the IRBs conduct reviews of investments Business Process Reengineering efforts.

Section 1072 states:

“Not later than one year after the date of the enactment of this Act, the appropriate chief management officer for each defense business system modernization approved by the Defense Business Systems Management Committee before the date of the enactment of this Act that will have a total cost in excess of $100,000,000 shall review such defense business system modernization to determine whether or not appropriate business process reengineering efforts have been undertaken to ensure that— (A) the business process to be supported by such defense business system modernization will be as streamlined and efficient as practicable; and (B) the need to tailor commercial-off-the-shelf systems to meet unique requirements or incorporate unique interfaces has been eliminated or reduced to the maximum extent practicable.

(2) ACTION ON FINDING OF LACK OF REENGINEERING EFFORTS. — If the appropriate chief management officer determines that appropriate business process reengineering efforts have not been undertaken with regard to a defense business system modernization as described in paragraph (1), that chief management officer— (A) shall develop a plan to undertake business process reengineering efforts with respect to the defense business system modernization; and (B) may direct that the defense business system
modernization be restructured or terminated, if necessary to meet the requirements of paragraph (1).”

The Deputy Chief Management Office provided interim guidance based on Section 901 of the Fiscal Year 2012 National Defense Authorization Act, stating: “To aid the DoD in making better investment decisions, Section 901 of the Fiscal Year 2012 National Defense Authorization Act (FY2012 NDAA) continues the refinement and evolution of the investment management process and establishes a single Investment Review Board (IRB)/Defense Business Council (DBC), chaired by the Deputy Chief Management Officer (DCMO) and expands the investment aperture. The IRB will provide an integrated, cross-functional enterprise view of defense business system investments for annual evaluation and funds certification.

The DCMO provides further implementation guidance: “It (the guidance) applies to DoD Components and other Defense Organizations, hereafter referred to as Components, and affects the obligation of funds, regardless of type, for Defense Business Systems that will have a total cost in excess of $1M over the period of the current future–years defense program. Defense Business Systems that require funds in FY 2013 and beyond will be reviewed using the new investment management process beginning in July 2012.”

DoD 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 IRBs 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 Business Enterprise Architecture, are being used to identify the sub-processes, systems, data standards, performance measures and laws, regulations, and policies necessary to improve our business and drive better IT implementations. This more holistic understanding will allow us to make more informed Enterprise-wide decisions.

DoD has already made progress in this area by focusing on process improvement first, and then ensuring the right tools and governance structures are in place. DoD Business Enterprise Architecture is maturing and serves as a tool that guides our investment decisions as well as aligning the Department to common standards and approaches. The investment management process provides 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 is delivering better results for the business operations Warfighters depend on.

DoD uses the end-to-end framework as a reference for rationalizing current business IT investments, and ensuring each investment supports the Department’s mission through enterprise architecture, the DoD business strategy. It is also being used to identify those investments that need to be terminated, integrated with another solution or sunset.

6.6.4 Strategic Sourcing

The Department of Defense has made great strides in realizing efficiencies in IT. During March 20, 2012 testimony before the House Armed Services Subcommittee on Emerging Threats and Capabilities, the DoD CIO outlined some of these efficiencies. According to the testimony, “The Department of Defense has achieved cost avoidance estimated at over $3 billion over a 10 year period through our Enterprise Software Initiative (ESI). DoD organizations have achieved significant efficiencies in the purchase of software, hardware and services from the open market. This is achieved as a result of terms and conditions negotiated with vendors whose products appear in the ESI inventory. Our IT Enterprise Strategy and Roadmap emphasizes the increased use of commodity purchasing of hardware, software, and services as a major means of achieving efficiencies. Through the sharing of purchase agreements across organizations within the Department, we are able to minimize the number of purchase vehicles in use, further streamlining our IT acquisition processes.”

In the Department of Defense Information Technology (IT) Enterprise Strategy and Roadmap (ITESR), the DoD CIO estimates that IT consolidation can deliver efficiencies that result in “$3.2 billion to $5.2 billion over the Future Years Defense Program. Annual efficiencies in FY16 and beyond are estimated to be between $1.2 billion and $2.2 billion per year.”

Further, the DoD CIO 10 Point Plan to Modernize Department of Defense Information Technology outlines Strategic Sourcing as one of the 10 points.

“The objective of this DoD strategic sourcing initiative for IT commodities is to adopt the model being used by the leading private sector companies. These organizations view purchase cost savings as only one of the benefits of strategic sourcing. Additional benefits include compliance with standards, sustainability, security, energy efficiency, asset tracking, technology refresh, quality and achieving small business or other “good citizen” goals.” By maximizing the value of COTS IT products and services through coordinated acquisition efforts for products of the same or similar capabilities, DoD will further reduce the number of contract vehicles,

---

consolidate procurement actions, and enable a more common IT operational environment across
the DoD. The two major operational thrusts, to commence in the 4th quarter of FY12, are:

1. Establish DoD-wide enterprise license agreements (ELAs) for software, associated
   services, and cloud computing services from key publishers
   a. Consolidate spend on core COTS software products and services from software
      publishers with high DoD order volume to leverage scale for maximum volume
discounts.
   b. Coordinate requirements development across Components to select COTS
      software products that enhance interoperability and provide a common user
      experience, and implement DoD-wide ELAs. Reduce unique configurations
      within Components and move towards a standard operating environment across
      DoD.
   c. Leverage existing COTS software acquisition and management expertise within
      the DoD to minimize the need for new investments in personnel and
      organizational resources.

2. Consolidate commodity IT hardware procurements through a few select procurement
   vehicles
   a. Focus on IT hardware end-user items first: desktops, laptops, monitors, printers,
      and multi-function devices.
   b. Develop joint buying standards that address DoD performance, interoperability,
      and IT security imperatives while still providing sufficient latitude to
      accommodate some variance in DoD Components’ diverse mission requirements
      and operational environments.
   c. Identify or create a small number of commodity IT hardware procurement
      vehicles that are scoped for enterprise-level buys and institute the joint buying
      standards. Make their use mandatory for all commodity IT hardware
      procurements.

6.6.4.1 Approach and Plan for Enterprise IT Systems
DoD efforts to move to enterprise IT systems and consolidate commodity IT components such as
Email and identity and access management systems are ongoing. Two examples of this work are
the Army’s ongoing move to the Defense enterprise Email Service and DoD’s Identity and
Access Management (IdAM) efforts. The Army’s move to the Defense Enterprise Email Service,
provided by the Defense Information Systems Agency (DISA), eliminates the need to move
information from one email system to the next, a requirement of the current system. Enterprise
email allows access from any Army location and any Army device that is accessible to the
NIPRNET, the DoD’s Non-Secure Internet Protocol Router Network. The Enterprise Email
system will ensure user identity, improving overall security. It will also allow the warfighter to
coordinate mission efforts by sharing information with both internal (DoD) and external entities,
including federal agencies and mission and coalition partners.
DoD’s IdAM initiative will provide timely access to information using authentication infrastructure that provides Dynamic Access Control capabilities, granting authorized users access to information assets based on established enterprise identity attributes that contain biographical, contextual, and biometrics data. The DoD CIO has a critical role in synchronizing identity issues across the Department for application in all mission environments. Department-wide IdAM capabilities will replace today’s decentralized, manually-intensive, organizationally-unique, static access control mechanisms that are becoming increasingly inefficient and unresponsive to DoD access needs and complicate non-repudiation for insider threats.\(^{54}\)

Key DoD IdAM Initiatives include PK Enablement (PKE) of SIPRNet, cryptographic logon and enterprise access control, based on role and attribute. Enterprise access control would include automated account provisioning, an authoritative database for identity and persona and documenting the force structure for identity/organization linkage.

**6.6.4.2 Approach and Plan for IT Infrastructure**

DoD is working to realize efficiencies and consolidate commodity IT components. The DoD CIO testified to this work on February 17, 2012 before the Committee on Oversight and Government Reform Technology, Information Policy, Intergovernmental Relations, and Procurement Reform Subcommittee. She noted the following work already completed:

- The Army reduced the number of IT applications from 218 to 77 (65 percent reduction) during their BRAC move from Fort Monmouth, New Jersey, to Aberdeen Proving Grounds, Maryland. The Army Acquisition Domain has reduced the number of IT systems within that Portfolio from 114 in 2006 to 67 as of February 2012, a 41% reduction. The Logistics Modernization Program has sunset [sic] all 42 instances of the Army's Standard Depot System (SDS). Additionally, they have sunset [sic] all but one instance (7 of 8) of the Commodity Control Standard System (CCSS), a system comprised of 460 applications.
- The Navy has reduced by 50 percent the number of applications across its 21 functional areas – a reduction of 29,000 applications since 2003. Since 2008, the Navy has reduced 1,400 other applications and eliminated over 400 legacy networks.
- The Marine Corps has gone from 1,802 applications to 688 over the past one and a half years.
- The Air Force has also taken aggressive action as well, and reduced its IT budget request by $100 million. Air Force Materiel Command Headquarters has organized a tiger team committed to finding software application duplications and outdated systems that can be terminated with acceptable risk.\(^{55}\)

Further efforts are included in the DoD Mobile Device Strategy (see page 9).

\(^{54}\) Department of Defense Chief Information Officer Campaign Plan Summary, p. 13.

\(^{55}\) Oral Statement of Teresa M. Takai Department of Defense Chief Information Officer before the Committee on Oversight and Government Reform Technology, Information Policy, Intergovernmental Relations, and Procurement Reform Subcommittee, February 17, 2012.
6.6.4.3 Approach and Plan for Business Systems

DoD is working to consolidate business system components, such as financial and human resources management systems. In the DoD Defense Business Systems Investment Management Process Interim Guidance, the DCMO outlines these efforts. The guidance outlines the DoD shift to an investment review and certification approach that groups Defense Business Systems (DBS) into portfolios (by functions and sub-functions) to promote visibility across the DoD’s business mission areas (BMA). This eliminates redundancy and enhances interoperability of DBS and fosters an end-to-end view that enables integration across the DoD’s business enterprise. DoD is also developing functional strategies and aligning them to DoD strategic goals and priorities. The guidance also outlines development and use of Organizational Execution Plans that present DBS in portfolios at the component level aligned to functional strategies to promote efficiencies through increased flexibility, better value to the user, and a positive return on investment. Through the submission of organizational execution plans for review, evaluation and certification, a holistic investment management process will be achieved.56

6.6.4.4 Shared Services Plan

DoD has long-standing shared services, such as the Defense Finance and Accounting Service (DFAS), the Defense Travel System, the Defense Civilian Pay System and shared readiness and mission systems, and The Defense Information Systems Agency (DISA) provides the network, computing infrastructure, and enterprise services to support information sharing and decision making across DoD.

Our 2012 efforts, consistent with the M-12-10 requirement to "move at least two commodity IT areas to shared services (e.g. E-mail, collaboration tools, web infrastructure, etc.),” include two DoD shared service initiatives: The Unclassified Information Sharing Service/All Partner Access Network (UISS/APAN) and the General Fund Enterprise Business System (GFEBS).

UISS/APAN is an unclassified internet capability that allows DoD and its Components to collaborate and share information with external mission partners to aid humanitarian assistance and disaster response and stability operation events.

The pilot version of the service is operational and hosted at the Pacific Warfighting Center at U.S. Pacific Command. In addition to Pacific Command, it serves three other Combatant Commands: European Command, Africa Command, and Southern Command. In 2012, this service is migrating to a DoD enterprise infrastructure and enterprise rollout. DISA has assumed program management responsibilities for UISS/APAN, and is transitioning it to the Enterprise Service Center in September 2012. After this transition, the remainder of the Combatant Commands will be provided support.

The expected cost savings and cost avoidance for the DoD for UISS/APAN are estimated at $8-12 million per year over the period 2012-2017. This is in large part due to many duplicative unclassified information sharing efforts across the Combatant Commands, some of which have multiple systems for the same environment.


52

For Official Use Only
The GFEBS implementation involves standardizing all financial management and accounting functions across the Army. As a result, Army financial professionals will have access to more timely, reliable, and accurate information, which improves cost management and control, allows more time to perform financial analysis, and facilitates a more accurate understanding of the value and location of property. When it achieves full operational capability in 2012, GFEBS will provide a comprehensive system for all of the Army's financial and accounting functions, including:

- Cost management
- Financials
- Funds management
- Property, Plant and Equipment (PP&E) – Equipment & Assets
- PP&E – Real property
- PP&E – Plant maintenance
- PP&E – Project Systems
- Reimbursables; and
- Spending chain

When fully deployed in 2012, GFEBS will engage approximately 60,000 users at some 200 locations worldwide, and will improve operations at almost every Army organization and function. To date, GFEBS fielding has resulted in the retirement of 13 legacy systems. An additional six systems have been partially subsumed. Upon completion of GFEBS fielding, an additional 55 legacy systems will be retired and 39 systems partially subsumed. The cost savings/avoidance associated with GFEBS implementation is estimated to be $60M.

6.6.4.5 IT Acquisition Approach and Plan

Consistent with the M-12-10 requirement to "Consolidate commodity IT spending under the CIO," the DoD CIO’s 10-Point Plan for IT Modernization leverages strategic sourcing for IT Commodities. This enterprise strategic sourcing initiative for IT will allow DoD to gain economies of scale, improve effectiveness of IT throughout its lifecycle, and reduce total costs to the enterprise.

Consistent with the M-12-10 requirement to "Target duplicative systems or contracts that supply common business functions within an agency for consolidation in order to streamline processes and leverage the purchasing power of the agency,” the DoD Enterprise Software Initiative seeks to implement a software enterprise management process within DoD.

Additional benefits include compliance with standards, sustainability, security, energy efficiency, asset tracking, technology refresh, quality, and achieving small business and other good citizen goals. The initiative will enhance current DoD bulk purchasing efforts by ensuring a focus on the larger set of objectives that can be realized from strategic sourcing.

Consistent with the M-12-10 requirement to "Establish targets for commodity IT spending reductions and deadlines for meeting those targets," the DoD CIO has set a goal of saving a
minimum of 15 percent at purchase and another 15 percent over the next two years after purchase.

To accomplish these objectives, the DoD CIO will leverage the existing Strategic Sourcing Board of Directors as a DoD Commodity Council. The Council will be co-chaired by senior leadership of Acquisition Technology and Logistics/Defense Procurement and Acquisition Policy and DoD CIO and will have representation from each of the Services. This Council will review requirements and analyze current DoD spending data to identify and agree on a DoD-wide strategic sourcing strategy for IT hardware and software.

Lastly, once strategic sourcing has been standardized across DoD, the DoD Commodity Council will implement a process for enterprise-wide strategic sourcing for commodity IT purchases. The Council will review and analyze current IT hardware spending and identify a standard set of hardware for DoD-wide procurement and use.

6.7 Lessons Learned and On-Going Performance Measurement

In its Strategic Management Plan (SMP) for FY12-FY13, the Department of Defense establishes specific business goals that support the findings of the Defense Quadrennial Review call for business improvements. Goal owners oversee and monitor the progress of these activities through established internal mechanisms that govern business activities. The DoD CIO owns Goal 3 - to “build agile and secure information technology capabilities.” This goal aligns with objectives laid out in this plan.

Each of the SMP business goals is supported by key initiatives designed to achieve goal outcomes and measures, defined as “a standard or basis for comparison; an assessment using quantitative data or sometimes qualitative data, tracked incrementally over a specified period.”

A key initiative is executing the DoD IT Enterprise Strategy and Roadmap. Another, as outlined in our 10 Point Plan for IT Modernization, is to Strengthen the Oversight of Information Technology investments. Both of these align to ongoing efforts to create a more joint focused information environment.

Some of the measures outlined to achieve these key initiatives, which align with the objectives in this plan, include:

- Reduce data centers by 18 percent in 4QFY12 and an additional 12 percent in 4QFY13
- Implement Enterprise Services compliance reporting and oversight process.
- Strengthen the oversight of Information Technology investments.
- Establish Commercial Mobile Device policy

In accordance with the SMP, the DoD CIO oversees and monitors progress to achieve these goals.
7 Appendix 3: Line of Business Service Plan

Line of Business Service Plan; the Program Manager of each Federal-wide Line of Business will submit a Plan to OMB via the Managing Planner agency's CIO that addresses increasing the quality and update of the IT shared services that are provided through that LOB by the end of FY 2013. The LOB Plan will follow guidance provided in the IT Reform Agenda's 25-Point Plan and the IT Shared Services Strategy.

The Department of Defense is not a Federal Line of Business Owner.
8 Appendix 4: IT Shared Service Plan

DoD has long-standing shared services, such as the Defense Finance and Accounting Service (DFAS), the Defense Travel System, the Defense Civilian Pay System, and shared readiness and mission systems. The Defense Information Systems Agency (DISA) provides the network, computing infrastructure, and enterprise services to support information sharing and decision making across DoD.

Our 2012 efforts, which are consistent with the M-12-10 requirement to “move at least two commodity IT areas to shared services (e.g., email, collaboration tools, Web infrastructure, etc.),” include two DoD shared service initiatives: The Unclassified Information Sharing Service/All Partner Access Network (UISS/APAN) and the General Fund Enterprise Business System (GFEBS).

8.1 Unclassified Information Sharing Service/All Partner Access Network (UISS/APAN)

UISS/APAN is an unclassified internet capability that allows DoD and its Components to collaborate and share information with external mission partners to aid humanitarian assistance and disaster response and stability operation events.

The pilot version of the service is operational and hosted at the Pacific Warfighting Center at U.S. Pacific Command. In addition to Pacific Command, it serves three other Combatant Commands: European Command, Africa Command, and Southern Command. In 2012, this service is migrating to a DoD enterprise infrastructure and enterprise rollout. DISA has assumed program management responsibilities for UISS/APAN, and is transitioning it to the Enterprise Service Center in September 2012. After this transition, the remainder of the Combatant Commands will be provided support.

The expected cost savings and cost avoidance for the DoD for UISS/APAN are estimated at $8-12 million per year over the period 2012-2017. This is due in large part to many duplicative unclassified information sharing efforts across the Combatant Commands, some of which have multiple systems for the same environment.

8.2 General Fund Enterprise Business System (GFEBS)

The GFEBS implementation involves standardizing all financial management and accounting functions across the Army. As a result, Army financial professionals will have access to more timely, reliable, and accurate information, which improves cost management and control, allows more time to perform financial analysis, and facilitates a more accurate understanding of the value and location of property. It achieved full operational capability in July 2012 and provides a comprehensive system for all of the Army's financial and accounting functions, including:

- Cost management
- Financials
- Funds management
- Property, Plant and Equipment (PP&E) – Equipment & Assets
GFEBS engages approximately 60,000 users at some 200 locations worldwide, and improved operations at almost every Army organization and function. To date, GFEBS fielding has resulted in the retirement of 13 legacy systems. An additional six systems have been partially subsumed. Upon completion of GFEBS fielding, an additional 55 legacy systems will be retired and 39 systems partially subsumed. The cost savings/avoidance associated with GFEBS implementation is estimated to be $60M.
9 Appendix 5: Key Artifacts for the Department of Defense Enterprise Architecture

The Department of Defense (DoD) Enterprise Architecture (EA) is a federation of architectures that are developed and maintained at the Department, capability area, and Component levels. The associated DoD Architecture Strategy (found at https://www.intelink.gov/wiki/DoD_AS) describes these concepts. A wiki version of the DoD EA (https://www.intelink.gov/wiki/DoD_CIO/DoD_EA) provides the latest DoD EA-related information as well as a context for the architecture-related information, which is also shown in the tables below. Table E-1 contains links to additional key information about the DoD EA and associated EA descriptions.

Table E-1. Key Information about the Department of Defense Enterprise Architecture

<table>
<thead>
<tr>
<th>Span</th>
<th>Artifact Name</th>
<th>Artifact Location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DoD Information Technology Portfolio Repository (DITPR)</td>
<td><a href="https://ditpr.dod.mil/">https://ditpr.dod.mil/</a></td>
</tr>
<tr>
<td></td>
<td>DoD Information Enterprise Strategic Plan and Roadmap (SP&amp;R)</td>
<td><a href="https://www.intelink.gov/wiki/Portal/DoD_IE_Strategic_Plan_and_Roadmap">https://www.intelink.gov/wiki/Portal/DoD_IE_Strategic_Plan_and_Roadmap</a></td>
</tr>
<tr>
<td></td>
<td>GIG 2.0 Documents</td>
<td><a href="https://www.intelink.gov/wiki/Global_Information_Grid_2.0">https://www.intelink.gov/wiki/Global_Information_Grid_2.0</a></td>
</tr>
<tr>
<td>Department of Navy</td>
<td>DON Enterprise Architecture (EA)</td>
<td><a href="https://www.intelink.gov/wiki/DONEA#Officially_Released_Versions_of_DON_Enterprise_Architecture">https://www.intelink.gov/wiki/DONEA#Officially_Released_Versions_of_DON_Enterprise_Architecture</a></td>
</tr>
</tbody>
</table>

---

\(^{60}\) Some URLs have specific additional requirements for accessing the documents.
<table>
<thead>
<tr>
<th>Span</th>
<th>Artifact Name</th>
<th>Artifact Location</th>
</tr>
</thead>
</table>
# Appendix 6: Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APAN</td>
<td>All Partner Access Network</td>
</tr>
<tr>
<td>ASRG</td>
<td>Architecture and Standards Review Group</td>
</tr>
<tr>
<td>BCL</td>
<td>Business Capability Life-cycle</td>
</tr>
<tr>
<td>BEA</td>
<td>Business EA</td>
</tr>
<tr>
<td>BRM</td>
<td>Business Reference Model</td>
</tr>
<tr>
<td>C4I</td>
<td>Command, Control, Communications, Computers, and Intelligence</td>
</tr>
<tr>
<td>CAF</td>
<td>Common Approach to FEA</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CPM</td>
<td>Capability Portfolio Management</td>
</tr>
<tr>
<td>DARS</td>
<td>DoD Architecture Registry System</td>
</tr>
<tr>
<td>DAS</td>
<td>Defense Acquisition System</td>
</tr>
<tr>
<td>DCMO</td>
<td>Deputy Chief Management Officer</td>
</tr>
<tr>
<td>DIEA</td>
<td>Defense Information Enterprise Architecture</td>
</tr>
<tr>
<td>DISA</td>
<td>Defense Information Systems Agency</td>
</tr>
<tr>
<td>DISR</td>
<td>DoD Information Technology Standards and Profile Registry</td>
</tr>
<tr>
<td>DITPR</td>
<td>DoD Information Technology Portfolio Registry</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DoDAF</td>
<td>DoD Architecture Framework</td>
</tr>
<tr>
<td>EA</td>
<td>Enterprise Architecture</td>
</tr>
<tr>
<td>EAMP</td>
<td>EA Management Plan</td>
</tr>
<tr>
<td>EIE</td>
<td>EA and Includes</td>
</tr>
<tr>
<td>EISP</td>
<td>Enhanced Information Support Plan</td>
</tr>
<tr>
<td>ER</td>
<td>Enterprise Roadmap</td>
</tr>
<tr>
<td>ETP</td>
<td>Enterprise Transition Plan</td>
</tr>
<tr>
<td>ExBd</td>
<td>Executive Board</td>
</tr>
<tr>
<td>FEA</td>
<td>Federal Enterprise Architecture</td>
</tr>
<tr>
<td>FISMA</td>
<td>Federal Information Security Management Act</td>
</tr>
<tr>
<td>FY</td>
<td>Fiscal Year</td>
</tr>
<tr>
<td>GIG</td>
<td>Global Information Grid</td>
</tr>
<tr>
<td>GTG</td>
<td>GIG Technical Guidance</td>
</tr>
<tr>
<td>GTG-F</td>
<td>GIG Technical Guidance Framework</td>
</tr>
<tr>
<td>GTP</td>
<td>GIG Technical Profile</td>
</tr>
<tr>
<td>IAM</td>
<td>Interoperability and Supportability Assessment Model</td>
</tr>
<tr>
<td>IC</td>
<td>Intelligence Community</td>
</tr>
<tr>
<td>IE</td>
<td>Information</td>
</tr>
<tr>
<td>IEA</td>
<td>Information Enterprise Architecture</td>
</tr>
</tbody>
</table>
ISO
ISP Information Support Plan

J6
JCD&E Joint Concept Development and Experimentation
JCIDS Joint Capabilities Integration and Development System
JCPAT Joint C4I Program Assessment Tool
JCSFL Joint Common Systems Function List
JDDA Joint Deployment and Distribution Architecture
JIE Joint Information Environment
JROC Joint Requirements Oversight Council

KPP Key Performance Parameter

MA Mission Areas
MDR Metadata Registry

NR Net Ready

OMB Office of Management and Budget
OMG Object Management Group
ORA Operational Reference Architecture

PfM Portfolio Management
PM Program Manager
PP&E Property Plant and Equipment
PPBE Planning Programming Budgeting and Execution

SIPRNet Secure Internet Protocol Router Network
SP&R Strategic Plan and Roadmap

UAF Unified Architecture Framework
UISS Unclassified Information-Sharing Service

WEA Warfighting EA