Defense Information Systems Agency (DISA)

GIG Convergence Master Plan 2012

(GCMP 2012)
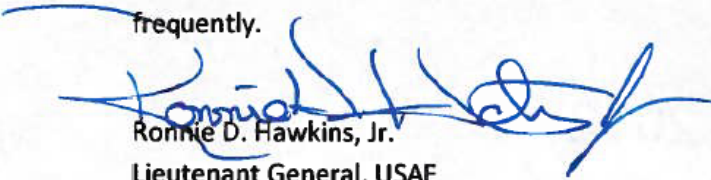
Volume I

02 August 2012

FOREWORD

The current political, economic, and technological climates are driving the Department of Defense (DoD) to provide more information technology (IT) capability to its users in a more secure manner with fewer resources. In order to achieve these high level goals, the Defense Information Systems Agency (DISA) must transform the way in which it delivers IT services. This Global Information Grid (GIG) Convergence Master Plan (GCMP) addresses this need by articulating the DISA technical strategy and providing a target technical architecture. The GCMP also includes the GIG Technical Baseline, which documents the approved set of DISA technical solutions. This version of the GCMP (GCMP 2012) builds on previous GCMP versions.

DISA's technical strategy is comprised of long-term, mid-term and short-term objectives, and a plan for achieving them. A key element of the plan is the target technical architecture, which differs from previous versions in that it is based on a cloud computing-centric model rather than a net-centric model. This shift in focus is deliberate, and intended to reflect the Department's adoption of cloud computing. Adopting this cloud computing-centric model also extends the notion of convergence to include a small number of well-defined interfaces for delivering service to DoD users worldwide through an increasing variety of end-user device types.

The GCMP 2012 also extends the organizational representation established in previous GCMP versions for managing services using a portfolio management construct. Service layers in the target technical architecture are made up of IT service portfolios that contain a set of service offerings. Program or project managers deliver the services, which provide capabilities to the DoD components and Communities of Interest (COI). DISA systems engineering processes, model based methods for precisely enumerating technical solutions, and technical documentation standards for service offerings are summarized.

DISA leadership will use portfolio management and the governance process described in this GCMP. The DISA Chief Engineers Panel will use the GCMP as a tool for technical governance and management of both the technical baseline and the technology roadmap. The DISA Component Acquisition Executive (CAE) will use the GCMP to ensure that integration points are identified across programs, capability releases are synchronized, and service offerings support DISA and DoD objectives.

Future versions of the GCMP will reflect updates to the DISA technical strategy. The target technical architecture will be updated annually as the DoD Platforms evolve. Additionally, the technical baseline will continue to be described by more and better models. Human readable forms of the models in standard technical documentation templates will be made available in electronic libraries, which will be updated frequently.

Ronnie D. Hawkins, Jr.
Lieutenant General, USAF
Director

Executive Summary

The Global Information Grid (GIG) Convergence Master Plan (GCMP) is the top-level document used for technical governance and management by the Defense Information Systems Agency (DISA). The GCMP is organized into two volumes. Volume I is strategically focused, defines the DISA technical strategy, and articulates the target technical architecture. Volume II is more tactically focused and provides a comprehensive technical reference; it consists of standard technical documentation templates for service offerings, the complete service offering to capability mapping, the complete DISA technical baseline, and the GIG Technical Guidance (GTG).

The Department of Defense (DoD), as part of its IT Effectiveness Initiatives, is defining a Joint Information Environment (JIE) in order to achieve three fundamental goals:
1. Provide more mission-enabling IT capability to users.
2. Increase security.
3. Improve efficiency.

The DISA technical strategy to achieve these goals is organized into long-term, mid-term and short-term objectives, and a plan to achieve them.

Long-term objectives:
1. Move to a commercial-government hybrid cloud computing environment with DoD retaining the identity provider role.
2. Improve service interoperability across core, intermediate and tactical edge environments.

Mid-term objectives:
1. Develop feasible methods, when using commercial cloud service providers, which protect data in transit and at rest, authenticate users, and apply appropriate access controls.
2. Provide virtual container technologies supporting secure unclassified operating environments on a wider variety of approved end-user devices.
3. Extend the DoD platforms to provide services for coalition enclaves.

Short-term objectives:
1. Provide a more efficient and capable set of common user services and platform services through consolidation of infrastructure and existing software licenses already purchased by DoD components.
2. Provide two private clouds: an unclassified DoD Platform, and a classified DoD Platform.
3. Improve end-user device access by migrating end-user applications to a web based interface and migrating end-users to a Virtual Desktop Interface (VDI) environment.

These objectives will be achieved through implementation of IT service portfolios and associated management controls. These IT service portfolios will implement the target technical architecture, which consists of three cloud service layers: common user services, platform services, and infrastructure services. In addition, the target architecture includes mission assurance services and enterprise service management, which both provide services to the three cloud service layers.

Contents

1. Introduction

This document is Volume I of the two-volume Global Information Grid (GIG) Convergence Master Plan for 2012 (GCMP 2012). The GCMP is one of three top-level documents used to govern and manage the technical development within Defense Information Systems Agency (DISA):

   i. **The DISA Campaign Plan.** Articulates how DISA is organized into lines of operation (LoO) and joint enablers, defines strategic objectives, establishes initiatives, and aligns resources.

   ii. **The GCMP.** Defines the DISA technical strategy, articulates the target technical architecture, and documents the technical baseline for DISA service offerings.

   iii. **The Program Objective Memorandum (POM).** Describes the service offerings to be implemented and the financial resources required to do so.

1.1. Purpose

The GCMP's primary stakeholder is the DISA Chief Engineers Panel (CEP), whose members use the GCMP for technical governance and management. The CEP maintains a forward-looking innovative vision by periodically updating the DISA technical strategy and the target technical architecture. Additionally, the CEP ensures programs and projects are technically sound and in alignment with the agency's technical strategy by approving changes to the technical baseline.

Another primary stakeholder is the DISA Component Acquisition Executive (CAE). The CAE uses the GCMP to support the integration and synchronization of capability offerings to meet service portfolio requirements.

Other GCMP stakeholders include:

- The DISA Service Portfolio Board (SPB), which governs IT service portfolios.
- DISA information technology (IT) service portfolio managers, who use the GCMP's service offering to capability mapping to identify gaps and overlaps in IT service portfolios.
- IT service program and project managers, who use both the target technical architecture and the GIG Technical Guidance (GTG) to guide their development of service offerings, which are added to the technical baseline when approved by the CEP.

1.2. Background

GCMP 2012 is the third generation GIG Convergence Master Plan. The first GCMP, published in March 2006, was primarily focused on migrating applications, services, and networks to a common infrastructure based upon the Internet Protocol (IP) in support of net-centricity.

The second GCMP (Version 1.0), published in March 2011, extended the notion of convergence beyond IP-based services and included applications, services, and data; communications; information assurance; NetOps and enterprise management; and computing infrastructure.

GCMP 2012 builds on these previous versions by articulating DISA's technical strategy and providing a target technical architecture. The new architecture is based on a cloud computing-centric model and differs from previous GCMP versions, which were net-centric. The new architecture also focuses the notion of convergence on a few, well-defined interfaces for delivering service to DoD users worldwide through an increasing variety of end-user device types.

1.3. Document Structure

The GCMP is organized into two volumes. Volume I is strategically focused. It defines the DISA technical strategy and articulates the target technical architecture. The technical strategy is organized into long-term, mid-term and short-term objectives, and a plan to achieve them. The plan includes a structure for facilitating portfolio management; a Model-based System Engineering (MBSE) methodology for defining technical architectures; system engineering processes, including documents required for describing service offerings that are part of the technical baseline; and standards and technology management.

Volume II is more tactically focused. It contains standard technical documentation templates, the complete service offering to capability mapping, and a brief summary of every service offering in the entire DISA technical baseline along with hyperlinks to the corresponding technical documentation in an electronic library.

The appendices of Volume II contain a complete list of GIG Technical Profiles (GTP) with corresponding hyperlinks; the complete set of GTPs is called the GIG Technical Guidance (GTG). These appendices also contain linkages between the GCMP and other important documents, such as the DISA Campaign Plan.

2. Technical Strategy

The DoD JIE initiative has three fundamental goals:
1. Provide more mission-enabling IT capability to users.
2. Increase security.
3. Improve efficiency.

The DISA technical strategy to achieve these goals is organized into long-term, mid-term and short-term objectives, and a plan to achieve them.

Long-term objectives (section 2.1):
1. Move to a commercial-government hybrid cloud computing environment with DoD retaining the identity provider role.
2. Improve service interoperability across core, intermediate and tactical edge environments.

Mid-term objectives (section 2.2):
1. Develop feasible methods, when using commercial cloud service providers, that protect data in transit and at rest, authenticate users, and apply appropriate access controls.
2. Provide virtual container technologies supporting secure unclassified operating environments on a wider variety of approved end-user devices.
3. Extend the DoD platforms to provide services for coalition enclaves.

Short-term objectives (section 2.3):
1. Provide a more efficient and capable set of common user services and platform services through consolidation of infrastructure and existing software licenses already purchased by DoD components.
2. Provide two private clouds: an unclassified DoD Platform, and a classified DoD Platform.
3. Improve end-user device access by migrating end-user applications to the cloud and migrating end-users to a Virtual Desktop Interface (VDI) environment.

2.1. Long-term objectives

In the long-term, DoD components and COIs will complete the transition from providing common user services on their own intranets in favor of the more complete set of cloud-based service offerings in the DoD Platforms, which are defined in the short-term objectives below. Consolidation of the infrastructure will continue as DISA implements and manages the DoD Platforms and all their services from a smaller number of strategic locations. The network will be normalized to deliver IT services from a standard set of aggregation and peering points, which will provide a set of joint security boundaries and include behavior monitoring. Additionally, the security emphasis will begin to shift from perimeter protection to transactional information protection and granular end-to-end security controls to enable protected information exchanges within a variable trust environment. IT service portfolios will continue to evolve and include commercial wireless gateways and remote access services.

The first long-term objective supports a vision of reducing the number of environments associated with security classification to two – one unclassified and one classified. Whereas DISA will continue to provide a DoD Platform for classified information, the unclassified DoD Platform may be provided using a commercial-government hybrid cloud with the government maintaining the identity provider role. One or more commercial cloud service providers may implement and manage a federal government community cloud for unclassified data and competition would be used to drive down costs while providing scalable, available and secure services. Cost reduction will be realized through centralization of IA management; reduction of the number of platforms to be trusted; economies of scale of server procurement; and expanded virtual server utilization. Successful migration of the DoD Platform to commercial providers is dependent on managing security and aggregation classification concerns (see first mid-term objective below).

The second long-term objective is to improve service interoperability across core, intermediate and tactical edge environments. This objective will be realized by developing and implementing a strategy to migrate the DOD Platform services to adaptable applications and services that will dynamically adjust to end-user devices and the connectivity associated with them. Such applications will adapt their behavior to the current environment, providing the end user an environment-optimized Quality of Experience. Two frameworks will be developed to support this approach: an End-User Device (EUD) Framework and an Edge Framework[1]. The EUD Framework will describe classes of end user devices to which applications may adapt. The Edge Framework describes service environments for core, intermediate and tactical edge users, addressing the full spectrum of users from robustly-connected garrison-based users all the way to those deployed in the most challenging tactical environments. A general representation of EUD and Edge frameworks and how they will fit into the DoD Platform is shown in Figure 4.

As part of this strategy, it is desirable to develop future applications using a universal development environment (similar to iPhone/iPad and various Android platforms) that allows the application to run in a thin or thick client mode depending on the current operating environment. This approach will allow tactical edge or other limited connectivity users to run the application locally when required. The design solutions will leverage the benefits of stateful application server interactions to overcome many of the aspects of disconnected state, intermittent connectivity, and/or limited bandwidth (DIL) environments

---

[1] https://www.intelink.gov/wiki/GIG_EWSE_FY10_GIG_Joint_Tactical_Service_Guidance_IPT

commonly found at the tactical edge. Store and forward will be considered an extension of routine stateful information exchange in adverse environments.

2.2. Mid-term objectives

The first mid-term objective is to develop feasible methods, when using commercial cloud service providers, that protect data in transit and at rest, authenticate users, and apply appropriate access controls. This will position DISA for the support of commercial cloud providers in the long-term. This objective is directly related to solving interim challenges associated with getting to the "end state" when DoD applications can execute securely in a commercial cloud environment. Two primary security concerns of managing data in the commercial cloud are DoD's inability to know where data on the internal servers ultimately resides and classification issues due to data aggregation. A promising approach to mitigating the latter concern may be to use the commercial cloud to manage ciphertext (encrypted) data.

The second mid-term objective is to provide virtual container technologies (enabled by short-term objective #2) that will make it possible to provide secure unclassified operating environments on a wider variety of approved end-user devices. Consequently, users may be permitted to use their own end-user devices in unclassified DoD environments.

The third mid-term objective is to extend the DoD platforms to provide services for coalition enclaves. Combatant Commanders (COCOM) primarily conduct warfighting operations with coalition enclaves; consequently, it is appropriate to provide DoD Platform services for those enclaves.

2.3. Short-term objectives

DoD components are being asked to consolidate their IT capabilities and in some cases use DISA-provided facilities and IT services. The first short-term objective is to provide a more efficient and capable set of common user and platform services through consolidation of software licenses that DoD components have already purchased. A more complete set of common user services and platform services will provide DoD components with improved mission-enabling IT capabilities at a lower total DoD cost than those currently provided on their own intranets. This consolidation will allow DoD components to devote more of their component resources to their core missions.

DISA will also reduce duplication within its own infrastructure. Consolidation within DISA includes managing computing, storage, network, and facilities resources in a holistic way to enable automation of account provisioning and system configuration. Automation will drive down labor costs, which are a significant portion of the rates that DISA must charge for IT services. Consolidation and automation can be achieved through cloud computing on both the Non-classified Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet), which has the potential to address a number of inefficiencies[2]. Consequently, the second short-term objective is for DISA to provide private clouds[3] on the NIPRNet and SIPRNet for DoD using government owned or leased resources. These two private clouds are called the DoD Enterprise Information Environment Platforms, or simply the "DoD Platforms."

---

[2] *Federal Cloud Computing Strategy*, February 8, 2011
[3] *NIST Special Publication 800-145*, September 2011

To support the trend towards thin clients and virtual container technologies, the third short-term objective is to improve end-user device access by migrating end-user applications to the cloud and migrating end-users to a Virtual Desktop Interface (VDI) environment. This will allow user applications and data to reside on central servers versus local devices, enabling users to access their work via thin clients, thick clients or mobile device. Adopting virtualized application presentation services provides a more manageable and cost efficient environment. Centralized software updates and back-ups will result in lower administrative costs and decreased vulnerability. Since no data is resident on the end-user device, data at rest (DAR) encryption is simpler and less expensive. This centralization of applications and data provides the necessary infrastructure for support of virtual container technologies in the mid-term.

Increased use of thin clients in large numbers will also reduce operating costs. Some commercial applications can be redesigned to support thin clients (including the sub-class of thin clients called "zero clients" or "ultra-thin clients," which have a more limited operating system than a thin client, providing just enough firmware for network connectivity, display drivers and input-output processing). Thin client applications will be developed in accordance with the EUD and Edge Frameworks (see Section 2.1 and Figure 4).

2.4. Plan to achieve objectives

DISA will use portfolio management, systems engineering, and standards & technology management to achieve the long-term, mid-term and short-term objectives.

2.4.1. Portfolio Management

The DoD Platforms follow the structure of the National Institute of Standards and Technology (NIST) Cloud Computing Reference Architecture[4] and are described in the target technical architecture (section 3), which defines the portfolio organizing construct used as a basis for managing implementation and sustainment of the DoD Platforms. In this target technical architecture, the DoD Platforms are organized into service layers which contain a number of IT service portfolios. IT service portfolios, in turn, consist of a set of individual service offerings as illustrated partially across the top of Figure 1. The individual service offerings listed are those IT services being provided or planned. Each service offering will be provided by a program or project office and perform functions described in a corresponding service offering description document as explained in Section 2.4.2 and Table 1 . DISA-provided service offerings provide one or more required capabilities, as shown along the left side of Figure 1. These capabilities provide users and/or other IT services with the "ability to do something."

Stated a different way, the DISA portfolio organizing construct comprises the service offerings as depicted along the horizontal axis of Figure 1. The DISA requirements construct comprises the IT capabilities depicted along the vertical axis. Mapping DoD Platform service offerings (and their functions) to the desired capabilities is the primary methodology used to ensure DISA is providing appropriate capabilities to the DoD components and COIs. Figure 1 illustrates this management construct which maps what is needed (the capabilities grouped by capability areas), to what DISA is

---

[4] http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf

providing or will provide (the service offerings grouped into service portfolios). For each required capability, there should be at least one service offering in the target architecture that provides it. Otherwise, a service offering gap exists. More than one service offering providing the same capability may indicate unnecessary duplication, or opportunities to increase efficiency. Service offerings that do not map to any desired capability may be candidates for elimination, or indicate a gap in the required capabilities. Volume II of the GCMP 2012 contains the full mapping of DoD Platform service offerings to capabilities.
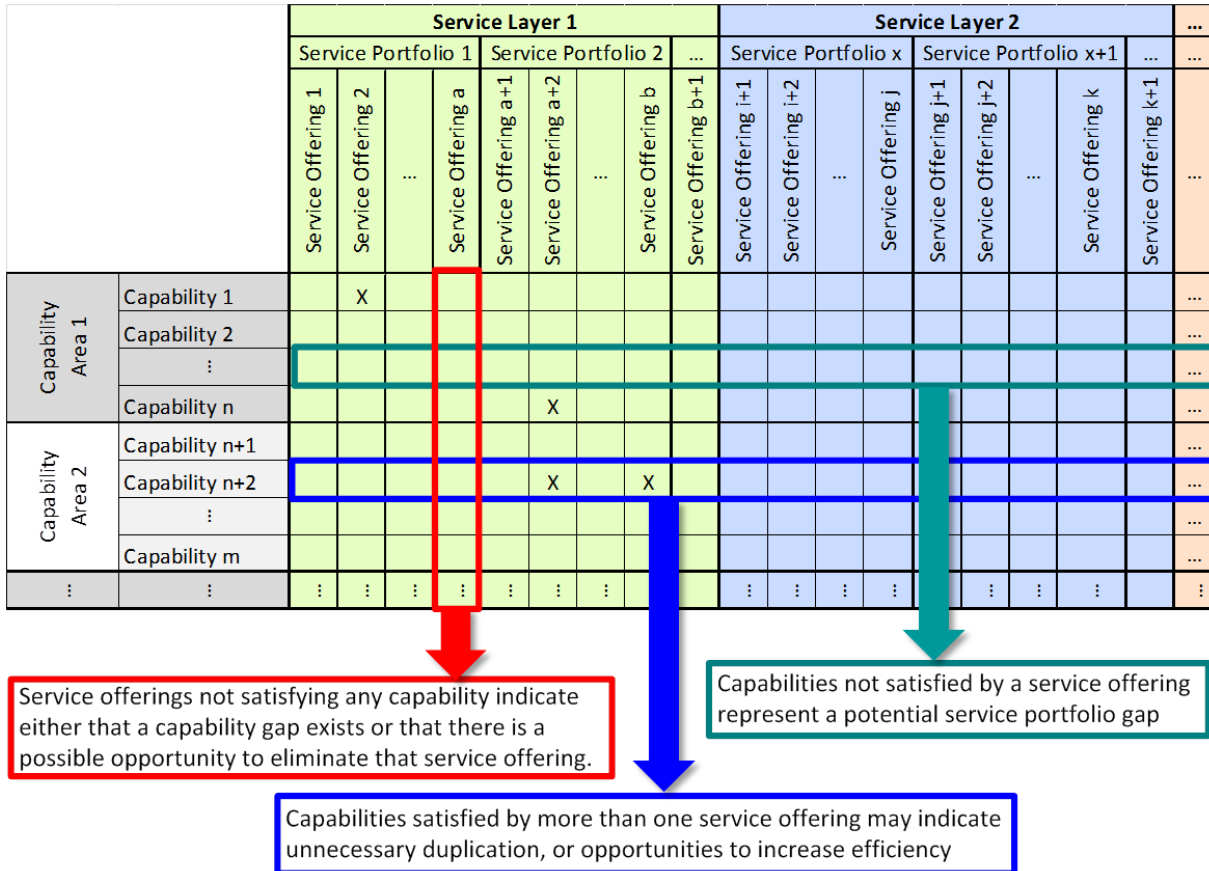
Figure 1. Service Offering to Service Capability Mapping

Portfolio management based on service offerings provides a straightforward way to determine service portfolio responsibility across DISA organizational boundaries. For most DISA portfolios, multiple DISA organizations provide service offerings. For example, the Program Executive Office for Mission Assurance (PEO-MA) provides the DoD Public Key Infrastructure (DoD PKI) and the Enterprise Services Directorate (ESD) provides enterprise-level authentication and access control services, both of which are part of the Identity and Access Management (IdAM) Services Portfolio. Additionally, some DISA organizations may provide an entire portfolio of service offerings; for example, the Network Services Directorate (NS) provides the entire Network Services portfolio.

An end-to-end service may span multiple service portfolios and/or organizational boundaries and therefore may require both internal and external Service Level Agreements (SLAs) to clarify the cooperation and governance for configuration control. On the other hand, a single DISA organization may provide an entire capability area. For example, the PEO for Command and Control Capabilities (PEO-C2C) is the only DISA organization that provides C2 capabilities.

Capabilities and services are developed and provided through the acquisition process. IT service requirements are governed by the DISA Service Portfolio Board (SPB). The SPB coordinates changes in service offerings with all the appropriate stakeholders and submits recommendations to the DISA Executive Committee (EXCOM). Implementation of the services is governed through the acquisition process with appropriate reviews and milestone decisions that incorporate independent assessments of design, operations, and testing. Service designs and technical solutions are evaluated by the DISA Chief Engineers Panel to ensure appropriate integration and architecture alignment. Operational readiness is assessed by the Net Readiness Review Board and JITC, as appropriate, to ensure effective service delivery, fielding, and sustainment.

2.4.2. Systems Engineering Processes and Model based Systems Engineering (MBSE)

The DISA systems engineering process[5] shown in Figure 2 was developed to ensure DISA services and applications are designed and built based on a common engineering approach and sound methodology that is in line with industry best practices and comply with DoD acquisition requirements. The system architecting process is part of the systems engineering process and exemplifies the required steps in the development of DoD Platform technical solutions. These solutions will be developed using an MBSE methodology in conjunction with the standards-based Systems Modeling Language (SysML), which focuses on the underlying data in the models. Figure 2 depicts the DISA MBSE process, where the system architecting process maps to the SysML diagrams that comprise the model. Models provide precise descriptions of how systems work and include well defined interfaces, which make it possible to combine existing models into end-to-end services; the models that make up these end-to-end services can then be used as patterns to develop new services. The DISA systems engineering process guide will be updated to describe such methods.

The model architecture organizes components based on overall system functional partitioning and delegates lower-level responsibilities to subordinate components. These models can be simulated to understand the system's behavior and performance, or can generate executable code that can be used to implement a service offering or application. The models also include test cases, which will be used to validate that requirements are being satisfied.

CEP-approved technical solutions will be documented in the technical baseline using three document types, each of which has a standard template[6]. Table 1 provides a brief description of each document type, which relate to the DISA MBSE Process as indicated on the right hand side of Figure 2. The

---

[5] DISA Systems and Software Engineering Process (DSSEP)
https://dashboard.disa.mil/SE_Reference_Manual_Version_6.3/Software1.htm
[6] The standard technical document templates:
https://east.esps.disa.mil/DISA/ORG/EE2/EE23/GCMP/SiteAssets/SitePages/GCMP%20Materials/TAD%20Template%20v1.4_6%20Feb2012.docx

documents describe the technical solution in human readable form, while the models embody the solution. The models will be stored in an electronic library. Automation tools will be used to generate artifacts and documentation from the models. For example, generation of the Technical Architecture Description and the Engineering Design Specification can be largely automated using such tools.
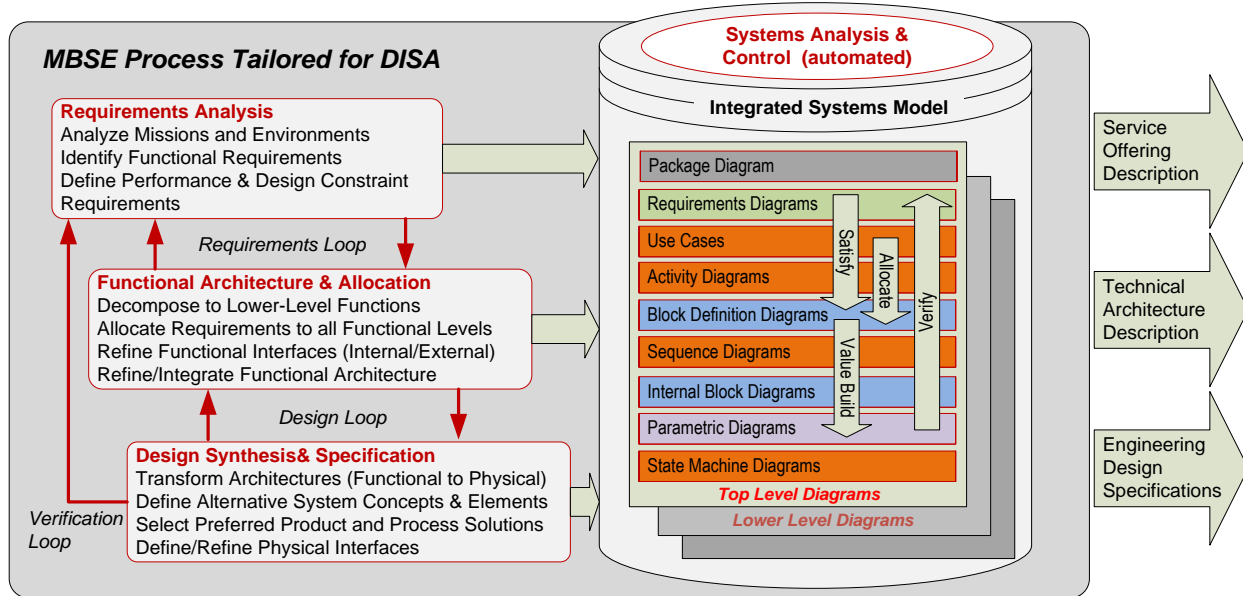

Figure 2. DISA Model-based system Engineering (MBSE) process

Table 1. Technical Solution Document Types

Document Type	Description
Service Offering Description	Documents the service offering at a high level and includes an operational concept (OV-1) drawing that illustrates the concept and addresses the major use cases, an explanation of the capabilities provided by the service, a high level functional architecture, a description of the business model, and service level objectives.
Technical Architecture Description (TAD)	Describes the technical solution associated with a service offering and documents the functional architecture. The TAD should be an excerpt from a model; it includes a summary of requirements, behavioral diagrams, structural diagrams, and some brief explanations to provide context. Additionally, interfaces to other services are enumerated.
Engineering Design Specification (EDS)	Documents the detailed design that will be used to implement the functional architecture. The EDS should be an excerpt from a model; it includes a summary of design decisions, including how the solution will scale, address data protection or security requirements, and meet service level objectives. It also specifies physical topology, hardware and software elements, and how they are to be configured.

The collection of approved technical solutions forms the GIG technical baseline, which is published in Volume II of the GCMP and will be updated frequently.

2.4.2.1. ITIL Service Design

Service design establishes governing IT practices, processes and policies in order to realize the IT strategy, facilitate the introduction of new IT services into the production environment, ensure quality service delivery, and increase customer satisfaction while ensuring cost-effective service provisioning. Service design includes both the design of new IT services and modifications to existing ones. Service design works in tandem with Systems Engineering (Figure 3) to identify service needs, map them to requirements for integrated services, and create the design specifications for the service assets needed to provide services. The following service design processes are part of the larger DISA Systems Engineering and Service Management processes[7]:

1. Design Coordination (Project Management): To coordinate all service design activities, processes and resources. Design coordination ensures the consistent and effective design of new or changed IT services, service management information systems, architectures, technology, processes, information and metrics.
2. Service Catalog Management: To ensure that a Service Catalog is produced and maintained, containing accurate information on all operational services and those being prepared to be run operationally. Service Catalog Management provides vital information for all other Service Management processes: Service details, current status and the services' interdependencies.
3. Service Level Management: To negotiate Service Level Agreements with the customers and to design services in accordance with the agreed service level targets. Service Level Management is also responsible for ensuring that all Operational Level Agreements and Underpinning Contracts are appropriate, and to monitor and report on service levels.
4. Risk Management: To identify, assess and control risks. This includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats.
5. Capacity Management: To ensure that the capacity of IT services and the IT infrastructure is able to deliver the agreed service level targets in a cost effective and timely manner. Capacity Management considers all resources required to deliver the IT service, and plans for short, medium and long-term business requirements.
6. Availability Management: To define, analyze, plan, measure and improve all aspects of the availability of IT services. Availability Management is responsible for ensuring that all IT infrastructure, processes, tools, roles etc. are appropriate for the agreed availability targets.
7. Continuity Management: To manage risks that could seriously impact IT services. It ensures that the IT service provider can always provide minimum agreed Service Levels, by reducing the risk from disaster events to an acceptable level and planning for the recovery of IT services. IT Continuity Management should be designed to support Business Continuity Management.
8. Information Security Management: To ensure the confidentiality, integrity and availability of an organization's information, data and IT services. Information Security Management usually forms part of an organizational approach to security management which has a wider scope than the IT Service Provider.

---

[7] Refer to the appropriate process owners for additional details about processes

9. Compliance Management (Quality Assurance): To ensure IT services, processes and systems comply with enterprise policies and legal requirements.
10. Architecture Management: To define a blueprint for the future development of the technological landscape, taking into account the service strategy and newly available technologies.
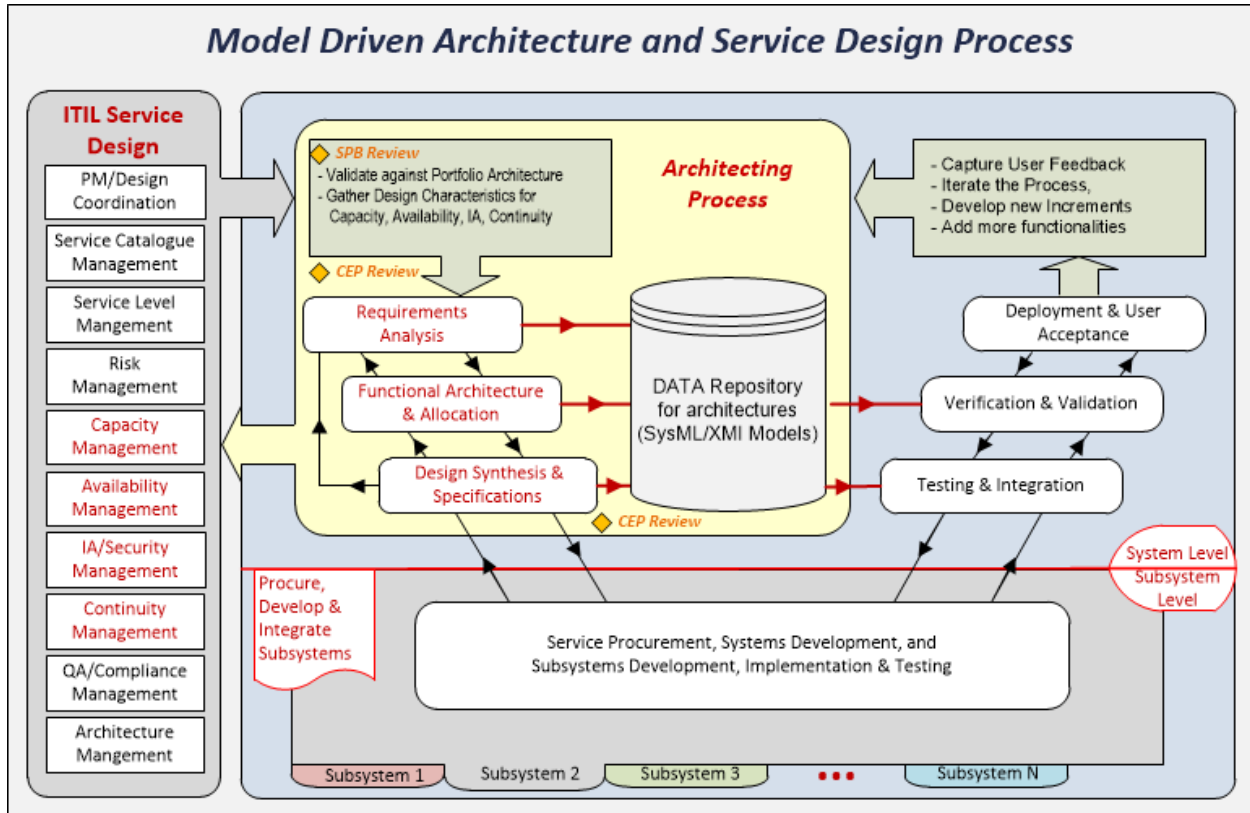

Figure 3. The DISA Systems, Software Engineering and Design Process

2.4.3. Standards and Technology Management

The plan for achieving technical objectives relies on using evolving standards, which will continue to be documented in the DoD IT Standards Registry (DISR)[8]. The DISR is enforced and quality-controlled by Enterprise Engineering (EE3). The DISA Chief Technology Officer (CTO) will oversee DISA's technology management activity, which will be supported by a Technology Management Framework (TMF[9]) to assist in developing and maintaining DISA's technology roadmap. DISA programs and projects will employ technologies that are consistent with the roadmap as they develop and evolve their technical solutions. Critical technology issues that address large numbers of users, that span program or domain boundaries, or that are associated with tactical environments, are addressed by the Enterprise Wide

---

[8] https://disronline.csd.disa.mil/
[9] https://tmf.csd.disa.mil/w/index.php/Technology_Management_Framework

Systems Engineering (EWSE) activity. EWSE performs technology assessments, studies appropriate technical issues, and publishes design guidance in the form of GIG Technical Profiles (GTP). The complete set of GTPs is referred to as the GIG Technical Guidance (GTG), which is documented in the GCMP Volume II.

2.4.3.1. Recognized DoD IT Issues and Challenges
The three aspects of standards and technology management described in the previous section provide a means for addressing key IT issues and challenges. The following is a current list of recognized DoD IT issues and challenges that must be addressed.

I. Information Assurance (IA) as it relates to managing risks associated with the use, processing, storage, and transmission of information and data, and the systems and processes used for those purposes

II. Tactical Edge communications and computing constraints related to the tactical and intermediate environments (disconnected or intermittent connectivity, limited throughput, high latency and jitter, and low-power requirements)

III. Mobile Communications & Computing and the explosion of end-user owned devices in the workplace, on the road and at home

IV. The increasing cost of IT infrastructure due to the proliferation of networks, computing, applications and end-user devices throughout DoD; and the resulting need for infrastructure consolidation at an enterprise level

V. The challenges in supporting legacy applications as DoD migrates to the cloud
   – Applications must be either sustained on their current environment, retired, or migrated to the cloud. The importance of this issue is underscored by the enormous investment in this space (> $1T).

VI. Information Security as it relates to data aggregation of unclassified information causing it to be sensitive or classified

VII. Providing real-time situational awareness, protection, and operational management (NetOps) in a holistic way

3. Target Technical Architecture
Implementation of the target technical architecture will achieve the second short-term technical objective to provide unclassified and classified private clouds for DoD using government owned or leased resources. These private clouds are the DoD Enterprise Information Environment Platforms, or simply the "DoD Platforms." The DoD Platforms follow the structure of the NIST Cloud Computing Reference Architecture and will be updated periodically to remain aligned with NIST standards. However, in this target architecture, the service layers have somewhat more general names that are more broadly applicable to the DoD. Additionally, some accommodations were made in the DoD Platforms for legacy service offerings and for Communities of Interest (COI) with special needs. For example, some COIs currently provide their own service offerings and potentially consume services from

all the service layers. DISA provides the services to support one DoD COI – the Command and Control & Information Sharing COI (C2&IS COI). Figure 4 illustrates the DoD Platform construct, which will be implemented in a common way on both NIPRNet and SIPRNet.

Convergence is an important GCMP theme; in this context, convergence means more than providing voice, video, and data applications with a single, common communications protocol. Rather, it embodies the cloud paradigm of providing services from each service layer to successively higher service layers in both DoD Platforms. This construct converges the DoD Platforms to a few, well-defined interfaces for delivering service. Furthermore, convergence in this context also embodies the notion that a service should be designed to accommodate all relevant end user devices and edge environments. As shown in Figure 4, frameworks for end-user devices and edge environments from core to tactical edge are an integral part of the service consumer layer (DoD Components and COIs). This underscores the importance of considering all relevant end user device and edge scenarios when designing services.
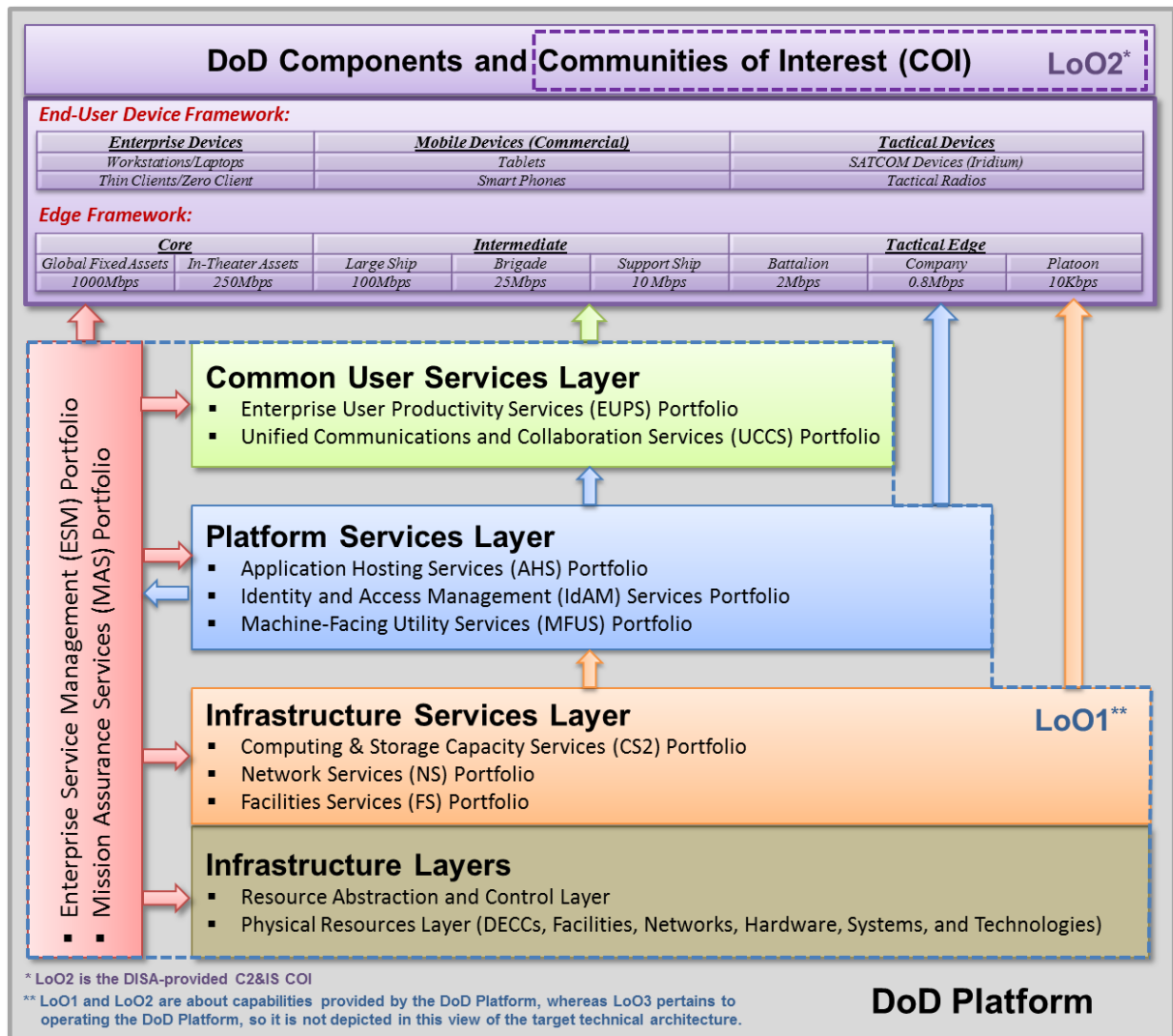

Figure 4. The Target Technical Architecture

The DoD Platforms also address the other short-term technical objectives. The first short-term objective requires a more complete set of common user services and platform services. Consequently, the common user services layer was updated to include more complete IT service portfolios that address both real time and non-real time user services. Similarly, the platform services layer was updated to provide a more complete set of portfolios.

The third short-term objective is to improve end-user device access, which requires enhanced mobility and resiliency. Because the Edge and End-User Device Frameworks are an integral part of each DoD Platform, technical solutions for service offerings can be tailored appropriately to address service delivery to end-user devices in tactical or non-tactical environments. This provides enhanced end user mobility (i.e. access to services regardless of location). Enhanced resiliency will be addressed in the technical solutions for each of the service offerings based on design guidance that will be published in one or more GIG Technical Profiles (GTP). The CEP must ensure that resiliency is addressed appropriately as part of the approval process for technical solutions.

3.1. Common User Services Layer

DISA adopted the term "Common User Services" to refer to the top-tier service layer of the target architecture. This service layer provides joint user-facing services of common interest across the DoD information environment, which is consistent with the NIST definition for cloud software as a service (SaaS). In general, common user services are classified by two factors, the first of which is whether or not they are real-time services. Real-time services are part of the Unified Communications and Collaboration Services (UCCS) portfolio; non-real time services are part of the Enterprise User Productivity Services (EUPS) portfolio. The second factor is whether implementation of the service offering can be *distributed* or whether the nature of the application or state of technology requires it to be *centralized*.

3.1.1. Enterprise User Productivity Services (EUPS) Portfolio

The Enterprise User Productivity Service (EUPS) portfolio is a set of non-real time IT service offerings. In 2011, DISA implemented two significant EUPS IT service offerings – Defense Enterprise E-Mail (DEE) Services and Defense Enterprise Portal Service (DEPS). Additionally, the EUPS portfolio includes content discovery services provided by the Intelligence Community's *Intelink* Management Office, which exposes discoverable DoD Platform data to users in accordance with their access privileges. DISA plans to implement additional EUPS IT service offerings, which include user storage and web-based office applications. Finally, the EUPS portfolio will include service offerings that distribute widgets and mobile software applications.

DEE is a service offering that provides three fundamental capabilities: electronic messaging (e-mail), calendaring, and people discovery in the form of a global persona directory. It is illustrative of the kind of application that can be implemented as a distributed system because users generally have a one-to-one relationship with their mailbox server. Consequently, end users can be provisioned to mailbox servers that are located close to them, which makes sense because the majority of e-mail traffic within most organizations is internal. Placing mailbox servers far from large concentrations of users affects both wide area network (WAN) resources and end user experience. The other factor that makes it

possible to implement DEE as a distributed system is the mechanism that mail clients use to discover their users' mailbox servers. The mail client has an auto-discovery feature that determines if the user's mailbox server is available, and if not, finds the backup mailbox server. This allows different users to be associated with different primary and backup mailbox servers on a per-user basis. Consequently, DEE was implemented as a distributed system.

In contrast, DEPS was implemented as a centralized system. DEPS provides a rich set of capabilities, which include document libraries, team rooms & calendars, wikis, blogs, user profiles, and personal sites for individual users. These capabilities are implemented on servers; in general, there is a many to one relationship between users and servers. Additionally, data is stored in databases and on file systems and must be replicated with backup instances. Whereas it is theoretically possible to synchronize two sets of data that are geographically distributed, the current technology for DEPS is not currently capable of doing so. The result is that DEPS will be implemented as a centralized system in the short-term.

3.1.2. Unified Communications and Collaboration Services (UCCS) Portfolio

As part of the Common User Services Layer, Unified Communications and Collaboration Services (UCCS) will be a suite of service offerings that provide integrated real-time communication services with a consistent unified user interface and user experience across multiple devices and media types. These services will include telephony (including IP telephony), video conferencing, instant messaging (chat), presence information, real-time data sharing (including web conferencing), call control, and speech recognition. Additionally, these services will be distributed or centralized depending on technology, mission needs, and performance requirements that affect end-user experience.

3.2. Platform Services Layer

As discussed in section 3 above and depicted in Figure 4 the DoD Platforms converge to a few, well-defined interfaces for delivering service. Each service layer provides service to other layers. The platform services layer has two sets of interfaces, the first of which provides platform services primarily for internal consumers, which include Common User Services, Mission Assurance Services (MAS), and Enterprise Service Management (ESM). The second interface type provides platform services for DoD components and COIs. Platform services are consistent with the NIST definition for cloud platform as a service (PaaS).

There are three platform services portfolios in the platform services layer – the Application Hosting Services (AHS) portfolio, the Identity and Access Management (IdAM) services portfolio, and the Machine-Facing Utility Services (MFUS) portfolio.

3.2.1. Application Hosting Services (AHS) Portfolio

The Application Hosting Services (AHS) portfolio provides hosting of user services and applications on standard computing platforms such as Windows and Linux. The AHS portfolio consumes services from the other platform services portfolios, which include IdAM services and MFUS. It also consumes computing, storage, network, and facility services from the infrastructure services layer. Computing and storage resources are organized into scalable blocks of configurable capacity and are connected to the

WAN using suitable network services, both of which are described in the infrastructure services layer below

Application hosting service offerings are delivered to two enclaves associated with each DoD Platform – production enclaves, which contain the DoD Platforms, and pre-production enclaves that contain pre-production environments used for validating technical solutions and testing updates. Each pre-production environment will include a complete duplicate of the corresponding DoD Platform and all its services, but in a separate pre-production enclave, and at an appropriately smaller scale. Validation and testing in the pre-production environment will become a required step for every DISA-provided service offering and every DISA-hosted DoD Component or COI service offering (including simple applications). Additionally, a full function development and test environment for individual applications will be provided and will utilize representative data and user loading for testing. The relationship of production, pre-production, and development & test enclaves and environment is shown in Figure 5.
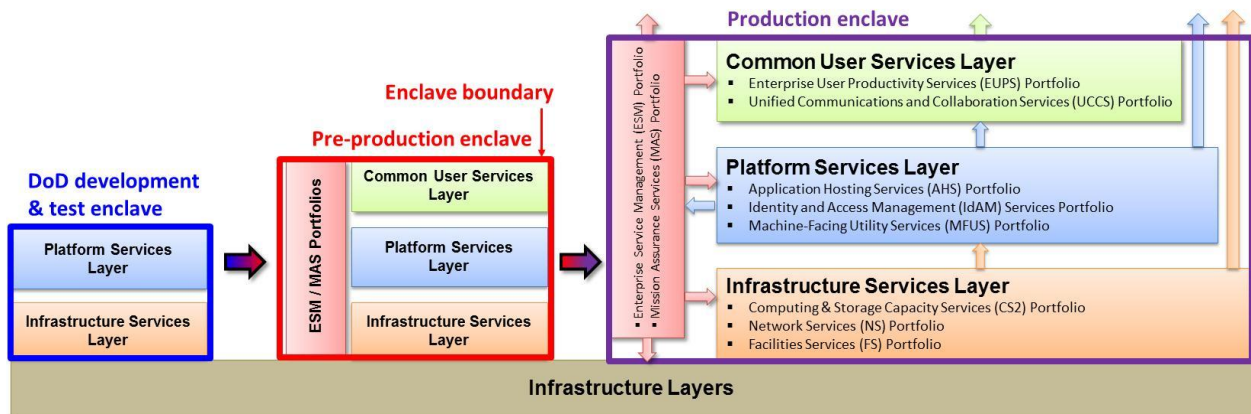

Figure 5. Production, pre-production, development & test enclaves and environments

File storage significantly affects both the performance and cost of most service offerings. Current file storage implementations are generally provided separately for each individual IT service offering. The Enterprise Storage Service (ESS) will consolidate these disparate storage services into an integral part of the AHS platform services in both DoD Platforms. The ESS will consist of centrally managed, distributed object stores in a multi-level structure.

Backup services and records management will be provided as part of the ESS for all common user services, MAS & ESM applications, and DoD-component & COI applications delivered using the AHS. Failover, continuity of operations (COOP), and backup retrieval capabilities are application specific, and therefore must be part of the design and implementation of each IT service offering.

3.2.2. Identity and Access Management (IdAM) Services Portfolio

The Identity and Access Management (IdAM) services portfolio provides two different, but related sets of functions: identities and their associated data, and how these identities and their associated data are used to manage access.

DoD established common standards to manage the end-to-end lifecycle of user identities and associated data across all enterprise resources both within and beyond the DoD information environment[10]. This common set of data includes standard DoD usernames, display names, and e-mail addresses on both NIPRNet and SIPRNet, along with additional identity, contact, and access control data. Collectively these data are known as "Enterprise User account data," which are managed for the DoD by the Defense Manpower Data Center (DMDC), and are available to DoD components on both NIPRNet and SIPRNet through the DISA-provided non-real-time Identity Synchronization Services (IdSS), as well as the DMDC-provided real-time Enterprise Identity Attribute Services (EIAS).

Access control is managed in one of two ways: account-based or attribute-based. For account-based systems, the IdSS synchronizes enterprise user account data from DMDC to DISA-provided and hosted IT service offerings. IdSS synchronizes directly to the Enterprise Application and Service Forest (EASF) and the Enterprise Authentication Gateway Services (EAGS). For other account-based DoD networks, IT devices, systems, applications and services that have their own access control systems, the IdSS Machine Interface (IdMI) provides and/or synchronizes enterprise user account data from the IdSS.

The EASF provides account-based authentication and access control and the global persona directory to DISA-provided common user services. The EAGS provide DoD authentication services to select DISA-hosted applications that are not able to directly authenticate users using the DoD's public key infrastructure (DoD PKI). Systems that use the EAGS will use their own access control (not the EASF).

Access control that uses data about a user from the source in real-time is termed attribute-based access control (ABAC). ABAC can be used by account-based systems, or when a system does not use accounts (does not maintain user state). DMDC provides the real-time EIAS for use in ABAC systems.

3.2.3. Machine-Facing Utility Services (MFUS) Portfolio

The Machine-Facing Utility Services (MFUS) portfolio provides registry, discovery, and mediation services for various data such as extensible markup language (XML) and metadata. This portfolio also provides service discovery and machine-to-machine messaging services.

3.3. Infrastructure Services Layer

The Infrastructure Services Layer consists of three IT service portfolios – Computing & Storage Capacity Services (CS2) portfolio, Network Services (NS) portfolio, and Facilities Services (FS) portfolio. These services portfolios bundle infrastructure resources into service offerings that can be consumed by the other service layers in the DoD Platforms. Infrastructure services are consistent with the NIST definition for cloud infrastructure as a service (IaaS).

DISA provides the services to support one DoD COI – the Command and Control & Information Sharing COI (C2&IS COI).

In some cases, it is appropriate to provide infrastructure service offerings directly to DoD components and COIs. For example, the Command and Control & Information Sharing COI (C2&IS COI) includes some

---

[10] *DoD Enterprise User Data Management Plan for Persons and Personas*, August 9, 2010

applications that are hosted and managed in other enclaves, and it is appropriate for DISA to provide infrastructure service offerings to support them. Another example relates to the DoD component intranets and COI networks; even if DoD leadership decided to move away from these intranets today, it would take years to implement. Consequently, it is appropriate for DISA to provide infrastructure service offerings that support these intranets as the DoD components and COIs transition to the DoD Platform. An example of where it is not appropriate to provide infrastructure services is for a DoD component that would like to use DISA facilities to host their own hardware and software that they operate – especially if the resources would be used to duplicate a DoD Platform IT service offering.

As illustrated in Figure 6, the infrastructure service layer is organized into a tiered hierarchy. At the highest level, DoD Platforms connect to external environments from a small number of high-level aggregation and peering points (AP1), which also provide security boundaries and centralized infrastructure services. AP1s will also be collocated with Internet access points (IAP), which connect the unclassified DoD Platform to the Internet and provide additional mission assurance services. A larger number of mid-level aggregation and peering points (AP2) provide security boundaries and distributed infrastructure services, which include support for DoD component intranets and COI networks. Some of the AP2s also include gateway services for tactical and wireless environments. End users are connected to the DoD Platform by end points (EP), which come in two types – tactical and non-tactical. Tactical end points (TEP) correspond to intermediate or tactical edge nodes in the edge framework. This tiered hierarchy provides context for a more detailed discussion of each of the infrastructure service portfolios, which is provided in the sections below.

3.3.1. Computing & Storage Capacity Services (CS2) Portfolio

High-level computing and storage capacity is provided at the DoD Enterprise Capability Centers (DECC), which are also the location of the high-level aggregation and peering points (AP1) and Internet access points (IAP). The DECCs include computing and storage capacity resources, which are organized into scalable utility blocks, called **Pods** that can be configured to provide any of the common user services, platform services, ESM and/or MAS. Mainframe capacity is also provided at the DECCs.

Mid-level computing and storage capacity is provided at the mid-level aggregation and peering points (AP2). The AP2s contain computing and storage resources, which are organized into similar scalable utility blocks as the DECC nodes (AP1), but with less capacity. These smaller computing and storage capacity resource blocks are called **mini-Pods**.

Tactical networks as defined in the edge framework are fundamentally different from networks that connect to core nodes in the edge framework because they use wireless resources somewhere in their communications infrastructure in order to serve environments characterized by a disconnected state, with intermittent connectivity, and/or limited bandwidth (DIL). Additionally, both intermediate and tactical networks that use satellite communications (SATCOM) resources have high latency in their WAN connectivity. Consequently, **tactical mini-Pods** need to be placed at appropriate locations in tactical enclaves. These tactical mini-Pods provide common user services and platform services to tactical enclaves regardless of the presence of WAN connectivity (discussed in section 3.3.2).
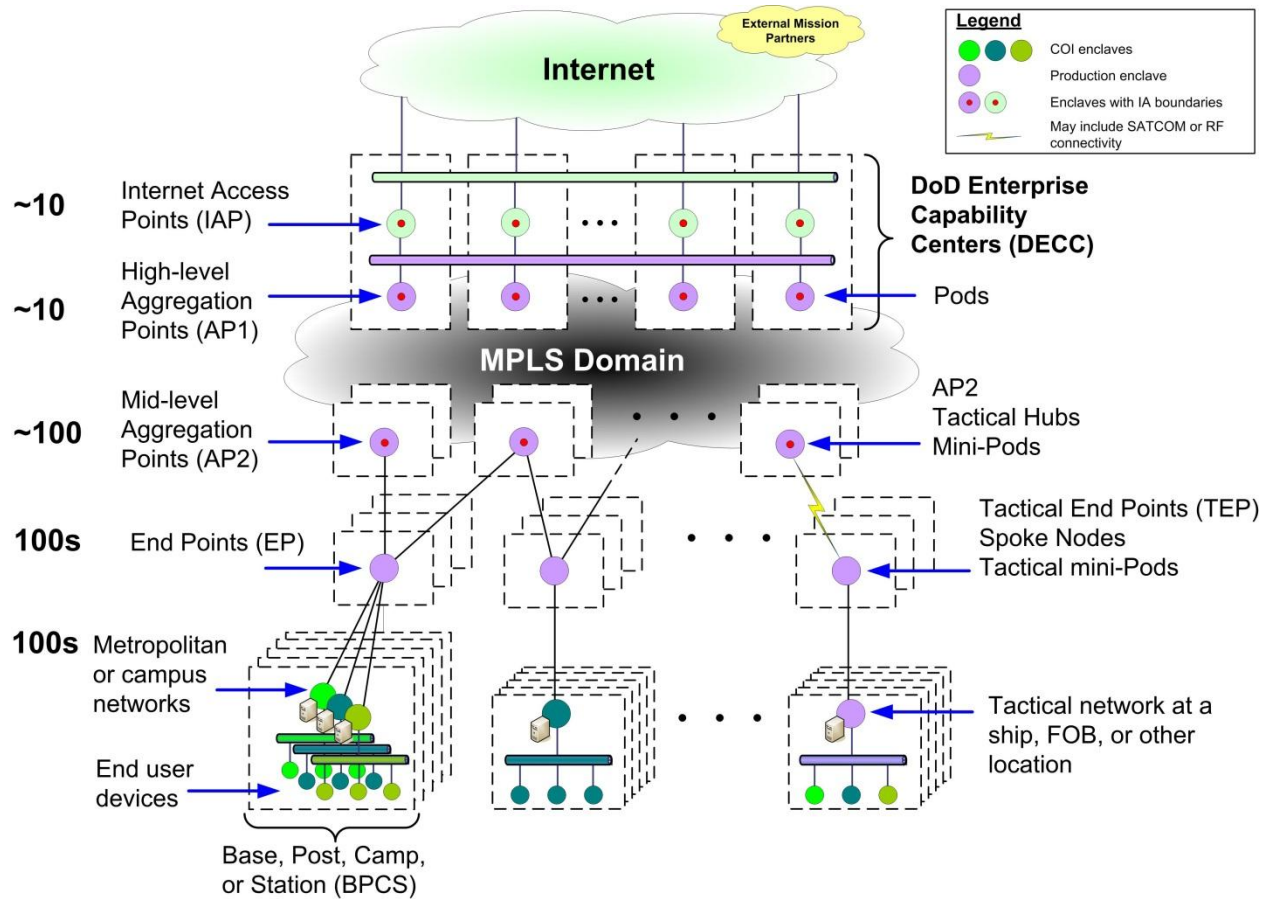
Figure 6. Tiered hierarchy that comprises the infrastructure services layer

All common user and platform services will be delivered from Pods, mini-Pods, or tactical mini-Pods at AP1s, AP2s, or TEPs. AP1s and AP2s have security boundaries and provide enclave gateway functionality. Consequently, DoD component intranets and COI networks that operate in a distinct enclave must peer with the production enclave at AP1s and AP2s.

3.3.2. Network Services (NS) Portfolio

The Defense Information Systems Network (DISN) is the common name for the collection of service offerings in the Network Services (NS) portfolio. The DISN is made up of DoD-owned and DoD-leased telecommunications networks and subsystems. DISA provides and operates the DISN, which provides services for all DoD mission areas. The DISN includes a rich set of service offerings that address a number of capability areas. The service offerings are organized into sub-portfolios, which include transport, data, SATCOM, and wireless[11].

The DISN architecture is hierarchical with a high speed optical transport core, a global packet switched backbone, and a multi-protocol service edge. Multi-protocol label switching (MPLS) provides virtual connections and traffic engineering, which support DoD component intranets and COI networks. The backbone transports information at all classification levels; Multi-protocol edge devices will exist at the

---

[11] DISN Overarching Technical Strategy (DOTS)

high-level aggregation and peering points (AP1), which are the centralized gateways, and mid-level aggregation and peering points (AP2), which are the distributed gateways depicted in Figure 6. There is a line of demarcation between NS and CS2 portfolios at AP1s and AP2s. The distinction is that the WAN resources are provided by the NS portfolio and local area network (LAN) resources are provided by the CS2 portfolio. Additionally, GIG Content Delivery Services (GCDS), which may include protocol optimization, compression, and caching functionality, are provided at AP1s, AP2s, and TEPs.

The multi-protocol service edge provides connectivity among tactical end points (TEP), non-tactical end points (EP), aggregation and peering points (AP1, AP2), DoD component intranets, COI networks, and end-user devices. Networks of different security classification levels may be cryptographically separated with IP encryptors at the edge of the network. The NS portfolio provides Quality of Service (QoS) for performance guarantees, IP multicast for efficient point-to-multipoint data communications, and Layer 2 and Layer 3 virtual private network (VPN) capabilities. Additionally, data capabilities include network timing, Domain Name System (DNS) for automated IP address resolution, and IP encryptor discovery.

The NS portfolio also includes fixed and mobile SATCOM service offerings, which may include gateway functionality. Gateway architectures are being standardized and will be provided at appropriate AP2s.

Wireless service offerings include support for new handheld mobile devices, applications and protocols. Implementation of a mobile device management service offering will enable DISA to manage mobile devices that access the DISN via commercial wireless networks.

3.3.3. Facilities Services (FS) Portfolio

To gain efficiency, resiliency, and improved user capabilities, facilities used for the DoD Platforms must be implemented and managed as a single service offering. The service offering consists of "power, space and cooling" for the CS2 and NS portfolios, and the facilities include the DECCs, and other locations where DoD Platform CS2 and NS capabilities exist.

3.4. Infrastructure Layers

The infrastructure layers depicted in Figure 6 support both DoD Platforms and include a resource abstraction and control layer and a physical resources layer. The distinction is that the abstraction and control layer virtualizes a variety of physical resources and provides a few standard interfaces to them. As the name implies, the physical resources layer refers to the actual resources themselves, which include DECCs, hardware, facilities, networks, systems, and technologies.

3.5. Enterprise Service Management (ESM) Portfolio

The Enterprise Service Management (ESM) portfolio provides a suite of capabilities used for

- Service monitoring and management
- Service status reporting
- Mission assurance
- Automation of service implementation and sustainment

ESM is an enterprise capability implemented as a common set of tools which will be used for all resource types (network services, and computing & storage services), and for all services offerings at all service

layers in the architecture (infrastructure, platform, common user, and mission assurance). This common tool set will instrument and automate the DoD Platforms, which will significantly reduce labor costs. The tool set will provide status views appropriate for the various help desks, service desks, operating centers, and end-user organizations. Additionally, ESM capabilities will include policy based methods.

3.6. Mission Assurance Services (MAS) Portfolio

The Mission Assurance Services (MAS) portfolio proactively maintains the confidentiality, availability, integrity, and non-repudiation characteristics of the DoD Platforms. In addition, they allow for dynamically allocating resources in accordance with mission technical requirements and priorities. At present, MAS is implemented via a complex set of overlapping and duplicative roles and responsibilities. The Joint Information Environment (JIE) Single Security Architecture (JIE-SA) is a multiphase approach that addresses this situation.

JIE-SSA comprises single security architecture that collapses the network security boundaries, reduces the external attack surface, and standardizes the management, operational and technical security controls to ensure the confidentiality, integrity and availability of DoD's information assets within all required mission contexts while also facilitating rapid attack detection, diagnosis, containment, and response.   Another high priority objective for JIE-SSA is to enable dynamic information sharing with DoD and its mission partners by shifting the focus from securing systems and networks to securing data and its use.

JIE-SSA will improve efficiency by reducing duplication of operations, establishing joint protections and responsibilities across COIs, leveraging other IT consolidation and enterprise-level capabilities, and flattening the network. Effectiveness will increase due to improved interoperability and information sharing with the ability to overlay COIs on the network across multiple regions, and to support non-traditional users such as mobile and embedded users. Security will improve through

- Division of the network into manageable and securable zones that align with enterprise specifications and enforce consistent, well-defined policies and procedures
- Placement of sensors at the most efficient locations for traffic capture and inspection
- Centralization and consolidation of the operations centers, tools, and personnel that monitor and defend the network

Appendix A   Acronyms

ABAC	Attribute-Based Access Control
AHS	Application Hosting Services
AP1	high-level aggregation and peering point
AP2	mid-level aggregation and peering point
ATIIP	Advanced Technology Identification and Insertion Process
BPCS	Base, Post, Camp, or Station
C2	Command and Control
C2C	Command and Control Capabilities
CEP	Chief Engineers Panel
COI	Community of Interest
COOP	Continuity of Operations
CS2	Computing & Storage Capacity Services
CTO	Chief Technology Officer
DECC	Defense Enterprise Capability Center
DECMS	Defense Enterprise Content Management Service
DEE	Defense Enterprise E-Mail Service
DEOAS	Defense Enterprise Office Application Service
DEPS	Defense Enterprise Portal Service
DESA	Defense Enterprise Security Architecture
DESS	Defense Enterprise Search Service
DEUSS	Defense Enterprise User Storage Service
DIL	Disconnected state, Intermittent connectivity, and/or Limited bandwidth
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	DoD IT Standards Registry
DISSEP	DISA Integrates Systems & Software Engineering Process
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DOTS	DISN Overarching Technical Strategy
DNS	Domain Name Service
EAGS	Enterprise Authentication Gateway Services
EASF	Enterprise Application and Service Forest
EDS	Engineering Design Specification
EIAS	Enterprise Identity Attribute Services
EP	End Point
ESD	Enterprise Services Directorate
ESM	Enterprise Service Management
ESS	Enterprise Storage Services
EUPS	Enterprise User Productivity Services
EUD	End-User Device
EWSE	Enterprise Wide Systems Engineering

FOB	Forward Operating Base
FS	Facilities Services
GCMP	GIG Convergence Master Plan
GCDS	GIG Content Delivery Services
GIG	Global Information Grid
GTG	GIG Technical Guidance
GTP	GIG Technical Profile
IA	Information Assurance
IaaS	Infrastructure as a Service
IAP	Internet Access Point
IdAM	Identity and Access Management
IdMI	IdSS Machine Interface
IdSS	Identity Synchronization Services
IP	Internet Protocol
IS	Information Sharing
IT	Information Technology
ITSMC	IT Service Management Council
JEDS	Joint Enterprise Directory Service
JIE	Joint Information Environment (JIE)
LAN	Local Area Network
LoO	Lines of Operation
MA	Mission Assurance
MAS	Mission Assurance Services
MBSE	Model-Based Systems Engineering
MFUS	Machine-Facing Utility Services
MPLS	Multi-Protocol Label Switching
MVNO	Mobile Virtual Network Operator
NetOps	Network Operations
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NS	Network Services
OV	Operational View
PaaS	Platform as a Service
PEO	Program Executive Office
PKI	Public Key Infrastructure
POM	Program Objective Memorandum
QoS	Quality of Service
SaaS	Software as a Service
SATCOM	Satellite Communications
SIPRNet	Secret Internet Protocol Router Network
SPB	Service Portfolio Board
SysML	Systems Modeling Language
TAD	Technical Architecture Description

TEP	Tactical End Points
TMF	Technology Management Framework
UCCS	Unified Communications and Collaboration Services
UML	Unified Modeling Language
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language