

UNCLASSIFIED

Department of Defense

**PDM III Core Enterprise Services  
Findings and Recommendations  
Report**



September 2006

Prepared by  
DoD CIO

UNCLASSIFIED

## 1 Introduction and Background

On December 20, 2005, Program Decision Memorandum (PDM) III tasked the Assistant Secretary of Defense for Networks and Information Integration /DoD Chief Information Officer (ASD[NII]/DoD CIO) as follows:

“(U) ASD(NII) in coordination with the Services, [Under Secretary of Defense (Intelligence)] USD(I), D(PA&E) and [Defense Information Systems Agency] DISA, conduct a study to assess the gaps and overlaps between DoD Component enterprise service programs. Provide assessment to the Deputy Secretary of Defense [DEPSECDEF] in July 2006.”

This report responds to this PDM III tasking with nine recommendations that provide the initial steps to accelerate the provisioning and adoption of Core Enterprise Services (CES) across the DoD. A cross-service working group was established, consisting of representatives from the Services, USD(I), D(PA&E), the Joint Staff and DISA to assist the review team with this report, which was conducted in two phases.

The first phase identified the seven major programs or activities thought to be developing Core Enterprise Services with the results documented in the 2006 CES Portfolio Review "Fact-Finding" Phase Results. This study assessed and categorized the core services capabilities being developed by these programs in a common framework based on the Net Centric Operations and Warfare Reference Model (NCOW-RM). The seven programs are:

1. DISA -- Net-Centric Enterprise Services (NCES)
2. Army -- Future Combat Systems (FCS) System-of-Systems Common Operating Environment (SOSCOE)
3. Air Force -- Distributed Common Ground System (DCGS) - Integration Backbone (DIB)
4. Global Combat Support System – Air Force (GCSS-AF)
5. Marine Corps Enterprise Information Technology Services (MCEITS)
6. Air Force Enterprise Information Technology Services (AF EITS)
7. National Security Agency (NSA) -- CASPORT.

The assessment was conducted by evaluating program documentation and performing interviews with members of the seven programs identified above, providing a snapshot of known efforts pertaining to CES. During the course of these interviews, the study team determined that AF EITS is a systems engineering activity with no program elements, so it does not appear in the findings and recommendations of this report. NCES was identified as the primary Program of Record (POR) to provide CES.

The second phase provides findings and recommendations based upon the phase one program assessments. This document contains the results of phase two. While the assessments only considered the seven programs listed above, the findings and recommendations impact all

DoD programs that are providing or consuming CES. The timeframe for this study did not permit side-by-side testing and evaluation of existing capabilities; however, the recommendations leverage the DoD's new Enterprise-Wide Systems Engineering (EW SE) activity to do so. This DISA-led EW SE activity is an engineering activity that focuses on identifying and resolving end-to-end issues related to the Global Information Grid (GIG). This activity includes direct participation by representatives from the DoD components.

This report is the first CES Domain portfolio review leading to the Enterprise Information Environment Mission Area (EIEMA) Investment Review Board (IRB). The process that is piloted in the development of this report will be the basis of an ongoing annual review of additional programs and activities in the EIEMA CES Domain.

## 2 Terms of Reference

The terms CES, gap, overlap, and federated CES are critical to understanding the findings and recommendations in this report. These terms are defined as follows;

1. Core Enterprise Services - a subset of Enterprise Services that is designed to provide a common information environment infrastructure. The services identified by the EIEMA will be mandated across the DoD. This will make other services in the enterprise visible and accessible to anticipated and unanticipated users. It also enables interoperability across the GIG and reduces duplication and unnecessary redundancy in the EIEMA portfolio.
2. Gap - an absence of a CES capability that has not been planned, resourced, or provided for a community of users on the GIG.
3. Overlap - a planned, resourced, or provided redundant CES capability.
4. Federated Core Enterprise Service - a core enterprise service (e.g., email) that is purposefully implemented according to an enterprise specification (e.g., SMTP) to aggregate value and enable local governance and accountability of the information. Federation participants agree to standards and policies and enforce them to deliver the aggregated value. For Federated CES, implementing specific standards and policies will be mandated by the DoD CIO.

## 3 Findings and Recommendations

The phase one study identified three gaps: 1) delivery of CES to tactical users, 2) enterprise service management for federated CES, and 3) standards-based interfaces for user-facing CES. The study also identified five overlaps: 1) credential validation, 2) authorization services, 3) enterprise directory services, 4) service discovery, and 5) presence awareness, instant messaging, and chat.

Each program in the study implemented capabilities based on the approved requirements documents. This is the first review of the capabilities across the portfolio. As a result, redundancies, and gaps that were not apparent before have now been identified.

The intent of the phase two findings and recommendations is to designate leads to define a small set of CES or standards and policies for federated CES to address the gaps and overlaps. Further, it is the intent of these findings and recommendations to establish a common interface definition for core enterprise services and standards on the NIPRNet, SIPRNet, and JWICS. Recommendations related to the "DoD Enterprise" should be interpreted to include services on all three networks, unless otherwise stated. Phase two results will be provided to EIEMA for implementation throughout the enterprise.

The DoD CIO, in coordination with the Director National Intelligence (DNI) CIO, shall direct and oversee execution of the following recommendations.

### **3.1 Publish DoD services strategy**

#### **3.1.1 Finding**

The DoD does not have a net-centric services strategy that establishes vision and goals. A net-centric services strategy will drive the enterprise to identify and adopt the necessary principles, standards, policies, and processes to evolve the DoD to an enterprise-wide service oriented architecture that would benefit the DoD and its partners.

#### **3.1.2 Recommendation**

OPR: DoD CIO. No later than 180 days after this report is approved, DoD CIO will publish a net-centric services strategy to provide the framework necessary to move the DoD to develop, reuse, and govern services.

### **3.2 Credential Validation**

#### **3.2.1 Findings**

The study identified overlap in credential validation services. Six of the programs that were reviewed are currently implementing or planning to implement credential validation services. In some cases, the credential is traditional userid/password, but other programs are using Public Key Infrastructure (PKI) certificates as the credential to support the mandate for two-factor authentication. Certificate validation capabilities provided by GCSS-AF and NSA CASPORT use the same COTS product on different networks. Further, the NSA COTS product is currently Protection Level-3 (PL-3) accredited. DoD PKI is currently providing certificate validation services on Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet).

Certificate validation is a critical component of PKI. All services and applications desiring to authenticate digitally signed messages or requests, and portals requiring

certificate-based authentication, require reliable and timely certificate validation. Many programs are developing services that are intended to be deployed on different networks (e.g., the Air Force's Distributed Common Ground System [DCGS-AF] on SIPRNet and Joint Worldwide Intelligence Communications System [JWICS]). Commonalities among certification validation architectures across network boundaries will eliminate the design and maintenance of custom validation solutions. This reduces the level of divergence as COTS components and custom software evolve over time. In addition, a single implementation ensures the same level of assurance, anywhere on a network, on the validity of a certificate.

### **3.2.2 Recommendations**

3.2.2.1 OPR: DISA, DIA. No later than 120 days after this report is approved, DISA and Defense Intelligence Agency (DIA) develop a plan of action and milestones (POA&M) to define and provide the credential validation services for the DoD enterprise. This POA&M will include a validation approach, deployment and resource plan, demonstration in Joint Expeditionary Force Experiment 08 (JEFX), and proposed migration paths for current security service providers, including DoD PKI, DoD Biometrics, NCES, GCSS-AF, CASPORT, Defense Enrollment Eligibility Reporting Systems (DEERS), and consumers (e.g., DCGS FoS, GCSS-AF, Net-Enabled Command Capability [NECC], and National System for Geospatial Intelligence [NSG]).

3.2.2.2 OPR: DISA, DIA. No later than 120 days after this report is approved and concurrent with the POA&M development, DISA and DIA, in conjunction with the Program Management Offices (PMOs) for DoD PKI, DoD Biometrics, NCES, DCGS FoS, GCSS-AF, NSG, DEERS, Integrated Shipboard Network System (ISNS), and CASPORT, will identify and document a common set of credential validation services for use on NIPRNet, SIPRNet, JWICS, with a consideration toward federal and coalition networks. All documentation should be delivered as service definitions that clearly describe the service interfaces and semantics of the services. The initial draft should be delivered to the Senior Systems Engineering Board (SSEB) for formal coordination and inclusion in the EW SE technical implementation guidelines.

3.2.2.3 OPR: DISA and DIA. Demonstrate the warfighter utility through joint experimentation of credential validation services with multiple PORs in JEFX 08 activities.

## **3.3 Authorization Services**

### **3.3.1 Finding**

Access control must be attribute-based and implemented in a consistent fashion to 1) manage access to resources across the DoD enterprise, and 2) enable machine-to-machine authorization of users across administrative and organizational boundaries (e.g. unanticipated but

authorized users). Authoritative data sources are required to provide the attribute data needed to support an enterprise Policy Decision Service.

This study identified overlap in the development of authorization services. Six of the seven programs reviewed are currently implementing, or are planning to implement, authorization capabilities; however, the range of products supporting this series of security services has a wide variance in maturity and risk. Access control mechanisms vary widely, ranging from tailoring portal contents to attribute-based access control mechanisms provided by CASPORT. Most are role-based.

POR Subject Matter Experts (SMEs) indicated that a key enabler for expanding information sharing is a common core enterprise authorization service. The DoD has started a migration toward Attribute-Based Access Control (ABAC).

### **3.3.2 Recommendations**

3.3.2.1 OPR: DISA and DIA. No later than 180 days after this report is approved, DISA and DIA will develop a POA&M to define and provide authorization services for the DoD enterprise. This POA&M will include a multi-program development and test environment, a validation approach, demonstration in JEFX 08, a deployment plan, and a resource plan. The POA&M shall include proposed migration paths for current security service providers (i.e., NCES, GCSS-AF, and CASPORT) and consumers (i.e., DCGS FoS, Defense Knowledge Online [DKO], and NSG) to begin using the enterprise authorization services and a proposed migration path for authoritative attribute sources to be made available to the authorization services.

3.3.2.2 OPR: DISA and DIA. No later than 180 days after this report is approved, and concurrent with the development of the POA&M, DISA and DIA, in conjunction with the PMOs for NCES, DCGS FoS, GCSS-AF, NSG, DEERS, ISNS, and CASPORT shall identify and document an initial set of authorization attributes, a process for introducing the use of this initial set of attributes, and the specifications for a common set of authorization services for use on NIPRNet, SIPRNet, and JWICS, with a consideration toward Federal and Coalition networks. All documentation should be delivered as service definitions that clearly describe the service interfaces and semantics of the services and the initial draft should be delivered to the Source Selection Evaluation Board (SSEB) for formal coordination and inclusion in the EW SE technical implementation guidelines.

3.3.2.3 OPR: DoD CIO. No later than 180 days after this report is approved, EIEMA shall engage DNI CIO and DoD Component CIOs to identify authoritative sources for authorization attributes within their areas of responsibility. In addition, EIEMA shall define the responsibilities of the authoritative sources.

3.3.2.4 OPR: DISA, DIA. In coordination with DoD Components, demonstrate warfighter utility through joint experimentation of the enterprise authorization services with multiple PORs in JEFX 08 activities.

### **3.4 Enterprise Directory Services**

#### **3.4.1 Finding**

An Enterprise Directory Service is needed to provide the DoD white pages (e.g., a single DoD enterprise directory that is the authoritative source for locator attributes). This directory service is necessary to enable the discovery of contact information for people throughout the enterprise. Authoritative data sources are required to provide the identity-related data (e.g., distinguishing attributes such as organization, role, and contact attributes such as phone number and email address) needed to support Joint Enterprise Directory Service (JEDS).

This study identified overlaps in the development of Enterprise Directories. Component Enterprise Directories are in various stages of development and implementation. However, identity locator attributes are not available to the DoD enterprise. Further, there is no consistent approach for DoD components to operate and populate identity attributes for their respective components and an approach for providing enterprise access to the component identity data does not currently exist.

#### **3.4.2 Recommendations**

3.4.2.1 OPR: DISA. No later than 120 days after this report is approved, DISA shall coordinate and publish a POA&M for implementing a JEDS on NIPRNet and SIPRNet. The POA&M shall include a detailed and coordinated deployment and resource plan, and a proposed migration path for the existing component directory services and the Intelink Full Service Directory (FSD). DIA will provide lessons learned and technology recommendations for the establishment of JEDS based on JWICS' enterprise directory services, and will advise and assist DISA as necessary in establishment of JEDS.

3.4.2.2 OPR: DoD CIO. No later than 120 days after this report is approved and concurrent with the development of the POA&M, DoD CIO shall coordinate with the DNI CIO, DoD Components, and Defense Manpower Data Center (DMDC) to identify authoritative sources for the 25 identity locator attributes defined by the DoD Active Directory Interoperability Working Group (DADIWG) within their areas of responsibility.

3.4.2.3 OPR: DISA. No later than 240 days after this report is approved, DISA shall define the interfaces for authoritative sources to provide locator attributes to the JEDS and provide the interface definitions to the SSEB for formal coordination and inclusion into the EW SE technical implementation guidelines.

3.4.2.4 OPR: DoD CIO. No later than 240 days after this report is approved, EIEMA to define responsibilities of authoritative sources for identity locator attributes. DoD CIO to task each Component CIO to implement a component directory service providing the functionality and interfaces defined in 3.4.2.3 above.

3.4.2.5 OPR: DISA. In coordination with DoD Components, demonstrate the warfighter utility of the Enterprise Directory Service through joint experimentation with multiple PORs in JEFX 08 activities.

## **3.5 Enterprise Service Discovery**

### **3.5.1 Finding**

This study identified overlap in the development of service registries. Each program assessed is deploying and populating its own service registry. Since April 2006, NCES supported two services registries: one part of the Early Capability Baseline (ECB) pilot environment and the other part of the Horizontal Fusion (HF) initiative. As of September 2006, only NCES Early Capability Baseline services were published in the ECB services registry, while more than 80 NCES and HF services were published in the HF Registry. While these two registries will be converged into a single service registry by October 2006, there is no single location on the network where developers in the DoD can publish and find services that are available for use on the GIG. No guidance exists for central publishing, federating distributed registries, or replicating a central registry locally.

Architecture decisions must be made concerning the enterprise service directory (e.g., federation vs. replication vs. central repository) so the policy can be appropriately written and programs can adapt accordingly. The Enterprise Service Directory is a key resource enabling service discovery and use on the GIG.

### **3.5.2 Recommendations**

3.5.2.1 OPR: DISA. No later than 120 days after this report is approved, DISA shall develop a POA&M to improve visibility and accessibility to the enterprise service registry currently at DECC Columbus on NIPRNET and SIPRNET (e.g., no human-in-the-loop, better user interface, etc.).

3.5.2.2 OPR: DoD Component CIOs. No later than 30 days after DISA completes service registry improvements in 3.5.2.1, Services/Agencies direct programs to populate the enterprise service registry on NIPRNet and SIPRNet with their services.

3.5.2.3 OPR: DISA. No later than 12 months after this report is approved and concurrent with the development of the POA&M, DISA, in coordination with DoD Components and DIA, define service registry guidance and discovery architecture. Guidance will address 1)

methodology to discover registry information across the Enterprise, 2) ways to bridge semantically similar concepts used in taxonomies across the enterprise, and 3) criteria for a federation hierarchy or a federated search approach to search the distributed registry. Initial documentation should be delivered to SSEB for formal coordination and inclusion in the EW SE technical implementation guidelines.

3.5.2.4 OPR: DoD CIO. No later than 30 days after DISA provides service registry guidance in 3.5.2.3, DoD CIO and DNI CIO publish policy guidance for programs to populate the enterprise service registry with their services, consistent with the registry architecture and guidance defined in 3.5.2.3.

## **3.6 Service Management**

### **3.6.1 Findings**

Several programs are implementing, or planning to implement, various service management capabilities, but there is insufficient information to determine whether this constitutes an overlap that should be resolved. The current approach is consistent with the NETOPS CONOPS service management strategy that states, "Services and Agencies will instrument their portions of the GIG in order to establish and maintain situational awareness," and "DoD components exercising management responsibilities for local or tactical GIG service delivery will comply with GIG reporting responsibilities." The NETOPS Community of Interest (COI) is currently defining the service management information that will be shared on the GIG.

This study identified a gap in enterprise service management capabilities. No program plans to provide a capability to monitor and manage Federated CES. Federated CES will consist of many services on different parts of the GIG acting cooperatively. To maintain situational awareness of the status of a given CES, the status of all cooperating services must be monitored and fused together. NCES Increment 1 service management capability will integrate with the Joint Task Force-Global Network Operations (JTF-GNO) or other Component Network Operations (NetOps) management capabilities to provide the situational awareness necessary to help prevent attacks and to ensure reliability and availability of critical components. In addition, service level metrics differ across the programs that were interviewed and there is no consensus on specifications and protocols required to make management and monitoring interoperable with the GIG NetOps capability.

To close this gap, the DoD must define the CES capabilities that are needed at the JTF-GNO and Command, Services, & Agencies (C/S/A) NetOps centers and other locations to implement the DEPSECDEF approved USSTRATCOM NetOps CONOPS. The NetOps COI is defining the information that PORs need to provide to those Capabilities.

### **3.6.2 Recommendations**

3.6.2.1 OPR: USSTRATCOM. No later than 90 days after this report is approved, USSTRATCOM will write a whitepaper describing the capabilities that JTF-GNO needs to manage the CES on NIPRNet and SIPRNet, including the federated CES.

3.6.2.2 OPR: USSTRATCOM and DIA. No later than 180 days after this report is approved, USSTRATCOM and DIA, working with DoD Components, will define an architecture, including a set of enterprise service management capabilities that should be provided as a CES. These capabilities shall include an initial service, or a suite of services, to provide enterprise service status reporting and a standard schema for passing service management information on NIPRNet, SIPRNet, and JWICS. Initial documentation should be delivered to SSEB for formal coordination and inclusion into the EW SE technical implementation guidelines.

3.6.2.3 OPR: USSTRATCOM, DISA, and DIA. No later than 12 months after this report is approved, USSTRATCOM and DISA, and DIA, supported by NetOps COI, complete a set of joint pilot activities and experiments with multiple PORs to demonstrate 1) the feasibility of the technical approach, and 2) the adequacy of the standardized schema for passing service management information, and demonstrated through a capability to provide service management of CES, including federates.

3.6.2.4 OPR: DoD CIO. No later than 60 days after completion of the joint experimentation in 3.6.2.3, DoD CIO will publish policy guidance based on the joint experimentation results for the use of the above architecture and schema across the GIG.

3.6.2.5 OPR: DISA and DIA. DIA will, in coordination with the DNI CIO, provide service management CES for JWICS. DISA will provide information on all aspects of NIPRNet and SIPRNet CES to DIA to ensure maximum reuse of technology and processes. DISA will ensure DIA is able to take advantage of enterprise licenses associated with NIPR/SIPR CES.

## **3.7 Standards for the Federation of IM, Chat, and Presence Awareness**

### **3.7.1 Finding**

Collaboration tools are widely available and the collaboration market is maturing. Major collaboration tool vendors have selected one of the following two competing standards to support with their tools: XMPP or SIP/SIMPLE. The programs assessed are either already implementing or planning to implement such collaboration suites. This is not an overlap since in some of these cases local implementation is required to support disconnected operation.

Instead, this study identified a gap in providing an enterprise capability for IM, chat, and presence awareness. These local implementations, however, do not have a single agreed-upon

standard for making presence awareness information available to the enterprise and conducting instant messaging and chat enterprise wide.

### **3.7.2 Recommendations**

3.7.2.1 OPR: DISA and DIA. No later than 120 days after this report is approved, DISA and DIA, in coordination with DoD Components, select and document an approach and service interface for making presence awareness information visible and accessible across the enterprise, and enabling enterprise-wide, IM, and persistent chat within a given network (i.e., NIPRNet, SIPRNet, and JWICS). The selected approach and interfaces shall be documented and delivered to SSEB for formal coordination and inclusion in the EW SE technical implementation guidelines.

3.7.2.2 OPR: DoD CIO. No later than 120 days after SSEB publishes technical implementation guidelines for IM/Chat/Presence Awareness in 3.7.2.1 above, DoD CIO publish policy guidance for use of the enterprise approach and interface standards as published in technical implementation guidelines.

## **3.8 Providing CES to Warfighters at the Edge**

### **3.8.1 Finding**

The phase one study identified a gap providing CES to warfighters at the tactical edge in the near term. NCES increment 1 will guarantee high performance service to users directly connected to a DISN Point of Presence (POP). Beyond the DISN POP, FCS/SOSCOE was the only program reviewed that provides a tactical CES solution specifically targeted to address the breadth of limited bandwidth and limited persistence transports, and other battle command requirements. Furthermore, planning and funding is not currently in place to deploy FCS/SOSCOE capabilities across all Army tactical units and platforms. There is currently no resourced plan that identifies how warfighters who are not reliably connected to DISN POPs, or FCS/SOSCOE-enabled networks, will have access to core enterprise services in the near term.

### **3.8.2 Recommendation**

3.8.2.1 OPR: Army and DISA. No later than 90 days after this report is approved, Army, and DISA will: convene a working group made up of representatives from the DoD Components and Agencies, including representatives from the following PORs (i.e., NCES, GCSS-AF, DCGS FoS, DIB, SOSCOE, ISNS and MCEITS PMOs), which shall characterize the CES gap between strategic, operational, and tactical networks, and deliver a plan to best address the CES gap on SIPRNet, including funding and executing a Capabilities-Based Analysis (CBA).

## **3.9 Standards-Based Interface for User-Facing NCES Services**

### **3.9.1 Finding**

This study identified a gap providing a standard interface to NCES services that provide a direct human interface. Six of the programs interviewed are providing portal or other service interfaces to their target audience, which includes both the end-user community and the developer community. There is no standard mechanism to provide end-user or developer with access to the NCES services from any of these portals or other services. For example, the NCES collaboration services should be packaged and available for implementation in any DoD portal, including Defense Knowledge Online.

A standard list of CES portlets that are available for use in any portal makes it easier to use the CES by both the developers and the end-users. Additionally, the availability of standard user interfaces to the CES enables program system developers to provide access to NCES services within their own system portals.

### **3.9.2 Recommendation**

3.9.2.1 OPR: DISA. Prior to Early User Test-3 for NCES, DISA will publish a set of standards-compliant user interfaces to provide end-user access to NCES services.

## Appendix A Glossary of Terms

<b>Access:</b>	To interact with a system entity to manipulate, use, gain knowledge of, or obtain a representation of some or all of a system entity's resources.
<b>Access Control:</b>	Protection of resources against unauthorized access. A process by which the use of resources is regulated according to a security policy and is permitted by only authorized system entities according to that policy.
<b>Attribute:</b>	A distinct characteristic inherent in, or ascribed to, an entity. An entity's attributes are said to describe it.
<b>Attribute-Based Access Control:</b>	A form of access control where authorization decisions and policies are based on attributes.
<b>Authentication:</b>	To confirm a system entity's asserted principal identity with a specified or understood level of confidence.
<b>Authoritative Source:</b>	A source of data that is recognized by appropriate governing authorities to be valid or trusted (e.g., the United States [U.S.] Postal Service is the authoritative source of U.S. mailing ZIP codes).
<b>Authorization:</b>	The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access.
<b>Authorization Policy:</b>	A set of one or more rules that governs access to a resource or class of resources.
<b>Credential:</b>	Data that is transferred to establish a claimed principal identity.
<b>Federation:</b>	A linking or binding of two or more entities together, each with like data, via a mutually agreed upon uniform policy and mechanism by which to format and share the data among the federation members.

**UNCLASSIFIED**

- Identity:** The collective set of attributes that defines an entity (i.e., subject, resource, etc.) within a given context.
- Service:** A mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description.
- Service Consumer:** An entity which seeks to satisfy a particular need through the use of capabilities offered by means of a service.
- Service Provider:** An entity (i.e., person or organization) that offers the use of capabilities by means of a service