

Net-Centric Implementation Framework

Part 1: Overview

Part 2: Traceability

Part 3: Migration Guidance

Part 4: Node Guidance

Part 5: Developer Guidance

**Part 6: Contracting Guidance for
Acquisition**

V 2.2.0

17 June 2008



Net-Centric Enterprise Solutions for Interoperability (NESI) is a collaborative activity of the USN Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I); the USAF Electronic Systems Center (ESC); and the Defense Information Systems Agency (DISA).

Approved for public release; distribution is unlimited.

Table of Contents

Perspectives	5
NESI Executive Summary	6
Part 4: Node Guidance	8
General Responsibilities	9
Nodes as Stakeholders	10
Net-Centric Information Engineering	11
Internal Component Environment	12
Integration of Legacy Systems	13
Coordination of Node and Enterprise Services	14
Coordination of Internal Components	15
Node Transport	16
Internet Protocol (IP)	17
IPv4 to IPv6 Transition	18
Mobile Nodes	20
Domain Name System (DNS)	21
Routers	22
Time Services	23
Mobile and Dynamic Networks	24
Multicast	25
Network Information Assurance	26
Enterprise Management Services	27
Virtual Private Networks (VPN)	28
Trusted Guards	29
Integration of Non-IP Transports	30
Black Core	31
Node Computing Infrastructure	32
Web Client Platform	33
Browser	34
Common Access Card (CAC) Reader	35

Web Infrastructure	36
Web Portal	37
Web Server	38
Web Application Containers	39
Host Information Assurance	40
Domain Directories	41
Instrumentation for Metrics	42
Node Application Enterprise Services	43
Overarching Issues	46
CES Definitions and Status	47
CES Parallel Development	50
CES and Intermittent Availability	51
Cross-Domain Interoperation	52
Net-Ready Key Performance Parameter (NR-KPP)	53
Information Assurance (IA)	54
Net-Centric Operations and Warfare Reference Model (NCOW RM)	55
Key Interface Profile (KIP)	56
Integrated Architectures	58
Core Enterprise Services (CES)	59
Directory Services	60
Security Services	62
Identity Management	

References 253

Perspectives

P1117: NESI Executive Summary

Net-Centric Enterprise Solutions for Interoperability (NESI) provides, for all phases of the acquisition of net-centric solutions, actionable guidance that meets DoD Network-Centric Warfare goals. The guidance in NESI is derived from the higher level, more abstract concepts provided in various directives, policies and mandates such as the Net-Centric Operations and Warfare Reference Model (NCOW RM) [R1176] and the ASD(NII) Net-Centric Checklist [R1177]. As currently structured, NESI implementation covers architecture, design and implementation; compliance checklists; and a collaboration environment that includes a repository.

More specifically, NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology (IT) portion of net-centric solutions for military application. NESI provides specific technical recommendations that a DoD organization can use as references. Stated another way, NESI serves as a reference set of compliant instantiations of these directives.

NESI is derived from a studied examination of enterprise-level needs and, more importantly, from the collective practical experience of recent and on-going program-level implementations. It is based on today's technologies and probable near-term technology developments. It describes the practical experience of system developers within the context of a minimal top-down technical framework. Most, if not all, of the guidance in NESI is in line with commercial best practices in the area of enterprise computing.

NESI applies to all phases of the acquisition process as defined in DoD Directive 5000.1 [R1164] and DoD Instruction 5000.2 [R1165] and to both new and legacy programs. NESI provides explicit counsel for building in net-centricity from the ground up and for migrating legacy systems to greater degrees of net-centricity.

NESI subsumes a number of references and directives; in particular, the Air Force C2 Enterprise Technical Reference Architecture (C2ERA) and the Navy Reusable Applications Integration and Development Standards (RAPIDS). Initial authority for NESI is per the Memorandum of Agreement between Commander, Space and Naval Warfare Systems Command (SPAWAR); Navy Program Executive Officer, C4I & Space (now PEO C4I); and the United States Air Force Electronic Systems Center (ESC), dated 22 December 2003, Subject: Cooperation Agreement for Net-Centric Solutions for Interoperability (NESI). The Defense Information Systems Agency (DISA) formally joined the NESI effort in 2006.

Content Structure

Perspectives	NESI Perspectives describe a topic and encompass related, more specific Perspectives or encapsulate a set of Guidance and Best Practice details, Examples, References, and Glossary entries that pertain to the topic.
Guidance	NESI Guidance is in the form of atomic, succinct, absolute and definitive Statements related to one or more Perspectives. Each Guidance Statement is linked to Guidance Details which provide Rationale, relationships with other Guidance or Best Practices, and Evaluation Criteria with one or more Tests, Procedures and Examples which facilitate validation of using the Guidance through observation, measurement or other means. Guidance Statements are intended to be binding in nature, especially if used as part of a Statement of Work (SOW) or performance specification.
Best Practices	NESI Best Practices are advisory in nature to assist program or project managers and personnel. Best Practice Details can have all the same parts as NESI Guidance. The use of

Part 4: Node Guidance

	NESI Best Practices are at the discretion of the program or project manager.
Examples	NESI Examples illustrate key aspects of Perspectives, Guidance, or Best Practices.
Glossary	NESI Glossary entries provide terms, acronyms, and definitions used in The context of NESI Perspectives, Guidance and Best Practices.
References	NESI References identify directives, instructions, books, Web sites, and other sources of information useful for planning or execution.

Releasability Statement

NESI **Net-Centric Implementation** v2.2 has been cleared for public release by competent authority in accordance with DoD Directive 5230.9 [R1232] and is granted Distribution Statement A: Approved for public release; distribution is unlimited. Obtain electronic copies of this document at <http://nesipublic.spawar.navy.mil>.

Vendor Neutrality

The NESI documentation sometimes refers to specific vendors and their products in the context of examples and lists. However, NESI is vendor-neutral. Mentioning a vendor or product is not intended as an endorsement, nor is a lack of mention intended as a lack of endorsement. Code examples typically use open-source products since NESI is built on the open-source philosophy. NESI accepts inputs from multiple sources so the examples tend to reflect whatever tools the contributor was using or knew best. However, the products described are not necessarily the best choice for every circumstance. Users are encouraged to analyze specific project requirements and choose tools accordingly. There is no need to obtain, or ask contractors to obtain, the tools that appear as examples in this guide. Similarly, any lists of products or vendors are intended only as references or starting points, and not as a list of recommended or mandated options.

Disclaimer

Every effort has been made to make NESI documentation as complete and accurate as possible. Even with frequent updates, this documentation may not always immediately reflect the latest technology or guidance. Also, references and links to external material are as accurate as possible; however, they are subject to change or may have additional access requirements such as Public Key Infrastructure (PKI) certificates, Common Access Card (CAC) for user identification, and user account registration.

Contributions and Comments

NESI is an open project that involves the entire development community. Anyone is welcome to contribute comments, corrections, or relevant knowledge to the guides via the Change Request tab on the NESI Public site, <http://nesipublic.spawar.navy.mil>, or via the following email address: nesi@spawar.navy.mil.

P1130: Part 4: Node Guidance

Part 4: Node Guidance is the fourth of six parts of the *NESI Net-Centric Implementation Document Set*. Part 4 provides a set of **Perspectives** which are a means of organizing and presenting information concerning nodes and encapsulating pertinent guidance and best practices. For more complete introductory information see the first part of this document set, *NESI Part 1: Overview* and the **NESI Overview** perspective [P1117].

A **Node** is a collection of **Components** (i.e., **systems**, applications, **services** and other Nodes) which results from the alignment of organizations, technologies, process, or functions. Potential alignment attributes include management, acquisition, mission, technological, sustainment, spatial, or temporal. A Node enables a common strategy for sharing the task of realizing net-centricity and interoperability. As a concept, Nodes may not necessarily be defined in terms of a concrete set of Components or size.

Note: *The use of the capitalized term **Node** in NESI Part 4, alone or preceded by the term **NESI** (i.e., **NESI Node**) differentiates the specific usage as defined in this perspective from the more general term **node**. A Node might be nested; such cases would likely introduce additional complexities that would require extra management attention and coordination.*

The presumption is that Nodes are actively managed. The shared capabilities necessary to support net-centric interoperability could be provided either by the Node or a system within the Node (i.e., the system is acting as executive agent for the capability).

The discussion of NESI Node guidance is presented in the following perspectives and is largely consistent with the DISA **Global Information Grid (GIG) Key Interface Profile (KIP) Framework (Draft v0.9)** [R1181].

- [General Responsibilities](#)
- [Node Transport](#)
- [Node Computing Infrastructure](#)
- [Node Application Enterprise Services](#)

The guidance and best practices in these perspectives is meant for those in a position to influence decisions regarding infrastructure and services provided by the Node for shared use by the systems within the Node. With respect to the GIG, the principal question addressed is how should a Node implement the shared infrastructure needed to achieve the DoD vision of broad integration and interoperability across the GIG, on behalf of systems within the Node, and in accordance with DoD policy and direction?

The guidance is applicable to information systems, such as those for command and control or intelligence. It may also be applicable, in part or whole, to other classes of systems or variants, such as embedded or real-time systems, but is aimed principally at systems that have desktop computers, **servers**, email, **Web browsers** and such.

Multiple operating environments are considered in the guidance including but not limited to fixed, deployed, mobile air/land/sea Nodes or other instance specific implementations. Occasionally, guidance may be provided for a specific environment or instance of a Node.

Factors such as physical environments and employment concepts directly influence the scope of a Node, and boundaries can vary widely. As a notional example, consider whether an individual foot soldier should be categorized as a Node. While soldiers are increasingly being outfitted with sensors and computing devices, it is unlikely (in the near term) that an individual soldier could host the requisite capabilities needed to ensure compliance with, for instance, the DoD **IA** Strategy including intrusion detection, **firewalls**, and such. Rather, a collection of soldiers such as an infantry battalion would be connected to a field command center that provides the requisite infrastructure. Note that this does not preclude an individual soldier from being directly addressable on the Global Information Grid (GIG), able to conduct information exchanges on a global scale. It simply means that requisite infrastructure is unlikely to be isolated to the soldier but rather shared with others. Likewise, nothing precludes the soldier from being a full Node should technology enable the soldier to carry all the requisite infrastructure elements.

P1131: General Responsibilities

In addition to the specific requirements of a Node to support transport, common computing infrastructure, **Enterprise Services** and **Community of Interest (COI) Services** there are some general responsibilities that a Node must support in order to ensure that the final product can interact with the rest of the **Global Information Grid (GIG)**. The responsibilities include the following:

- [Nodes as Stakeholders](#)
- [Net-Centric Information Engineering](#)
- [Internal Component Environment](#)
- [Integration of Legacy Systems](#)
- [Coordination with External Enterprise](#)
- [Coordination of Internal Components](#)

P1132: Nodes as Stakeholders

Formally represent a Node as a **stakeholder** in the acquisition and evolutionary activities of all the **Components** the Node will host. A Node's Component composition will change over time; maintain and identify all the known Components throughout the lifecycle of the Node. This action is fundamental to the provisioning of a shared infrastructure and the avoidance of functional duplication within the Node.

The necessity of a Node involvement as a stakeholder in its Components may not be obvious; it has a bearing on **Global Information Grid** (GIG) interoperability. Component independent planning and evolution is likely to result in the external exposure of inconsistencies or, worse, incomplete, inaccurate, or misunderstood data. Consider two systems within the Node that both ingest a particular type of data, but process it at different levels of fidelity, and are independently intending to publish the result to the rest of the GIG. This is an example of when a Node manager would want to work across the systems to ensure that the Node presents its collective capability clearly.

Guidance

- [G1569](#): Maintain a comprehensive list of all of the **Components** that are part of the Node.
- [G1570](#): Assume an active management role among the **Components** within the Node.

P1133: Net-Centric Information Engineering

Of particular concern for **Global Information Grid** (GIG) interoperability is the information contained in inter-nodal information exchanges. Information exchanges are typically the purview of the systems within the Node, rather than the Node itself, and the details are worked out by a **Community of Interest** (COI). But the Node infrastructure must be engineered to support information exchanges between various COIs. The COIs can require any number of Components to fulfill the mission. When a Component wishes to make its data available to the **enterprise**, there are different enterprise design patterns the Component can use. For example, the mechanism selected by a Component to exchange information may be publish-subscribe, broker, or client server. The Node infrastructure must support whichever enterprise design pattern mechanism is selected. Consequently, the Node has a stake in the Component design. Additionally, the Node has a stake in performance specifications provided in the **Service Level Agreements** (SLA). The Node must support the SLA contract with the Node's infrastructure.

Node management should designate COI representatives to track, advocate, and engineer information exchanges in support of the **DoD Net-Centric Data Strategy**. According to this strategy, "COI is the inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange." The principal mechanism for recording COI agreements is the **DoD Metadata Registry** required by the DoD CIO *DoD Net-Centric Data Management Strategy: Metadata Registration* memo. There are registry implementations on the **Non-Secure Internet Protocol Router Network** (NIPRNET), **Secret Internet Protocol Router Network** (SIPRNET), and **Joint Worldwide Intelligence Communications System** (JWICS).

The DoD Metadata Registry Web site (<http://metadata.dod.mil>) provides a search capability; there is also a **SOAP**-based interface to the Registry.

Guidance

- **G1571**: Maintain a comprehensive list of all the **Communities of Interest** (COIs) to which the **Components** of a Node belong.
- **G1572**: Include the Node as a party to any **Service Level Agreements** (SLAs) signed by any of the **Components** of the Node.
- **G1573**: Define the enterprise design patterns that a Node supports.
- **G1574**: Define which enterprise design patterns a **Component** requires.
- **G1575**: Designate Node representatives to relevant **Communities of Interest** (COIs) in which Components of the Node participate.

Best Practices

- **BP1865**: Provide sufficient program, project, or initiative **metadata** descriptions and automated support to enable **mediation** and translation of the data between **interfaces**.
- **BP1866**: Coordinate with end users to develop interoperable materiel in support of high-value mission capability.

P1134: Internal Component Environment

Nodes should provide an environment to support the development, integration, and testing of net-centric capabilities of their Components. As Nodes themselves and the Components within the Nodes move closer to the implementation of net-centric capabilities, it becomes increasingly important to provide a development, integration, and test environment to support those capabilities. This environment should allow for exercising the Node infrastructure and either hosting services locally within the Node or providing access to **Net-Centric Enterprise Services** (NCES). The particulars on how to do this depend on the characteristics of the Node. For example, mobile or deployed Nodes would provide environments substantially different than fixed land-based or permanent Nodes.

Specialized services will likely be hosted locally for Nodes in real-time, dynamic and mobile environments, such as those used for information exchange across the **Joint Airborne Network**. An emerging trend in the commercial networking/IT industry is to realize high performance capabilities with a combination of hardware-based (e.g., ASIC-driven) switches (e.g., XML router) and services (e.g., mediation). Commercial industry has experienced significant performance issues while running applications and services on the Internet, especially those that are XML-based.

When applicable, developers should be using the NCES piloted **Enterprise Services** offered by **DISA** for development, test, and integration at the earliest opportunity within the Node and Component lifecycles. In the absence of a Node-provided environment, Component developers should use the piloted services directory, through an early adopter agreement, but use of a Node-provided environment at the earliest opportunity is preferable to minimize problems. Potential causes of problems include security parameters, network configuration, and product inconsistencies.

DISA has published an "NCES Pilot Participants Guide" that describes the process for using the piloted services.

Guidance

- **G1576**: Provide an environment to support the development, build, integration, and test of net-centric capabilities.
- **G1577**: Maintain an **Enterprise Service** schedule for interim and final **enterprise** capabilities within the Node.
- **G1578**: Define a schedule for **Components** that includes the use of the **Enterprise Services** defined within the Node's enterprise service schedule.
- **G1579**: Define which **Enterprise Services** the Node will host locally when the Node becomes operational.
- **G1580**: Define which **Enterprise Services** will be hosted over the **Global Information Grid** (GIG) when the Node becomes operational.

P1135: Integration of Legacy Systems

Nodes might contain systems or **applications** that are in the **Sustainment** lifecycle phase. These **Components** are often referred to as **legacy** systems or applications. Changing the internals of such Components to support net-centricity is impractical and often has little return on investment. Usually, the decisions to brand a system or an application as a **legacy system** is made at a high level in conjunction with the operational user and acquisition communities. When the legacy functionality needs to be exposed as an interim solution internally to a Node or external to the Node as a **proxy** it is often accomplished using a service that uses a **facade** technique. The facade technique is often implemented using a wrapper or an adapter **design pattern** around the existing legacy system or application.

Guidance

- [G1581](#): Expose **legacy system** or **application** functionality through the use of a service that uses a **facade design pattern**.

P1136: Coordination of Node and Enterprise Services

The **Net-Centric Enterprise Services** (NCES) capabilities under definition, development, or in pilot testing are complex and use leading edge technologies. The status, availability and deployment schedule for services should be reflected in an integrated master schedule for the Node that shows planned dependencies of systems within the Node on these services. Given the rate of evolution and leading edge nature of some services, the coordination of efforts should be detailed, including specific version numbers, workarounds, assumptions, constraints, configuration, and best practices. Note that these practices should be followed for coordination with both external and Node-provided **Enterprise Services**.

Guidance

- **G1577**: Maintain an **Enterprise Service** schedule for interim and final **enterprise** capabilities within the Node.
- **G1578**: Define a schedule for **Components** that includes the use of the **Enterprise Services** defined within the Node's enterprise service schedule.
- **G1582**: In Node **Enterprise Service** schedules, include version numbers of standard Enterprise Services interfaces being implemented.

Best Practices

- **BP1865**: Provide sufficient program, project, or initiative **metadata** descriptions and automated support to enable **mediation** and translation of the data between **interfaces**.

P1137: Coordination of Internal Components

The shared infrastructure provided by Nodes, for shared use by its member **Components** cannot evolve independently of the Components within the Node. Nodes may host a variety of Components and Components may be members of multiple Nodes. Consequently, the development of Components is likely to occur with differing timeframes and rates of evolution. This presents a coordination challenge for the Node managers.

Guidance

- [G1583](#): Provide routine **Enterprise Services** schedule updates to every **Component** of a Node.

P1138: Node Transport

A Node provides a transport infrastructure shared among the **Components** within the Node, implements **Global Information Grid (GIG) IA** boundary protections, and is **Internet Protocol Version 6 (IPv6)** capable. In some cases, guidance may seem rudimentary, but history demonstrates that configuration errors for such rudimentary aspects are often the cause of interoperability, integration, and **information assurance** issues.

The **DISA/National Security Agency (NSA) Security Technical Implementation Guide (STIG)** documents are applicable in several places throughout this section. The guidance those documents provide is not repeated here. The STIG documents are updated frequently as new vulnerabilities are discovered and the current "state of the art" is refined. Consult the applicable STIG documents and monitor them periodically for updates as a fundamental part of design activities.

Transport elements a Node provides are obviously essential in achieving net-centricity but also play a key role in minimizing interoperability issues. The following perspectives describe several Transport elements:

- [Internet Protocol \(IP\)](#)
- [Domain Name System \(DNS\)](#)
- [Routers](#)
- [Time Services](#)
- [Mobile and Dynamic Networks](#)
- [Multicast](#)
- [Network Information Assurance](#)
- [Enterprise Management Services](#)
- [Virtual Private Networks \(VPN\)](#)
- [Trusted Guards](#)
- [Integration of Non-TCP/IP Transports](#)
- [Black Core](#)

Note: *The elements described above are in a recommended order of implementation, with the basic enablers described first, for a notional Node. Specific elements and implementation order may vary according to factors such as Node connectivity, scale, mission, and concepts of employment.*

Guidance

- **G1584:** Provide a transport infrastructure that is shared among **Components** within the Node.
- **G1585:** Provide a transport infrastructure for the Node that implements **Global Information Grid (GIG) Information Assurance (IA)** boundary protections.

Best Practices

- **BP1704:** Consult the applicable **Security Technical Implementation Guidance (STIG)** documents as a fundamental part of design activities, and monitor the STIGs periodically for updates.

P1139: Internet Protocol (IP)

The **Assistant Secretary of Defense for Networks and Information Integration**, ASD(NII), includes adapting Internet and World Wide Web constructs and standards with enhancements for mobility, surety, and military unique features (e.g., precedence, preemption) as one of nine [Net-Centric Attributes](#). The **Internet Protocol** (IP) is among the most fundamental of protocols needed for **Global Information Grid** (GIG) interoperability. There are, however, a number of interoperability challenges emerging as DoD usage of IP networking continues to expand. Two of these areas are the following:

- [IPv4 to IPv6 Transition](#)
- [Mobile Nodes](#)

P1140: IPv4 to IPv6 Transition

A 9 June 2003 **ASD(NII)**/DoD CIO memo, *Internet Protocol Version 6 (IPv6)*, is the first in a series of memos (see the References below) addressing DoD transition to **IPv6** and establishing IPv6 as the next generation network protocol for DoD with the transition date goal of FY 2008. The DoD IPv6 Transition Office created in DISA is responsible for master transition plan development, acquiring **Internet Protocol** (IP) addresses, providing necessary infrastructure and technical guidance, and ensuring that unified solutions are used across DoD to minimize cost and interoperability issues. DoD components are tasked with the development of the component transition plans and with providing guidance and governance to programs. Three main Milestone Objectives (MOs) have been outlined for the gradual and controlled transition of the **enterprise**. Currently only those systems approved as MO1 pilots are allowed to switch to IPv6 in operational environments.

To enable this transition, as of 1 October 2003 all **Global Information Grid** (GIG) assets being developed, procured, or acquired shall be IPv6 capable (while retaining compatibility with IPv4). The **DoD IPv6 Working Group** is working on IPv6 implementation issues through formal standards bodies. A high level working definition for "IPv6 capable" is available; the list of the standard IPv6 specifications approved for the use in DoD networks is hosted on the **Defense IT Standards Registry** (DISR) Web site.

Prepare an IPv6 transition plan for the Node infrastructure as well as the transport users within the Node in coordination with the **Component** and DoD transition plan; the Node IPv6 transition plan is subject to review and approval by the appropriate IPv6 transition authority. Coordination is essential to ensure that the intermediate network infrastructures are IPv6 capable in the planned timeframe, and similarly for other-end network infrastructures for known system interfaces. The Node's IPv6 transition plan should consider applicable DoD Component IPv6 transition plans, IPv6 working group products, and include interoperability testing in the plan. The net-centric concepts of loose coupling and discoverable services may be impacted by the transition to IPv6 if services begin depending on IPv6-specific features. Identify services developed to utilize IPv6 features and which may perform differently if accessed via an **Internet Protocol Version 4** (IPv4) infrastructure.

IPv6 transition has an impact on many transport infrastructure components. The IPv6 Transition Plan for a Node should include transition of all impacted network elements including **DNS**, routing, security, and dynamic address assignment. The *DoD IPv6 Network Engineer's Guidebook* (Draft) and the *DoD IPv6 Application Engineer's Guidebook* (Draft) provide guidance for transition of impacted components.

Guidance

- **G1586**: Provide a transport infrastructure for the Node that is **Internet Protocol Version 6** (IPv6) capable in accordance with the appropriate governing transition plan.
- **G1587**: Prepare an **Internet Protocol Version 6** (IPv6) transition plan for the Node.
- **G1588**: Coordinate an **Internet Protocol Version 6** (IPv6) transition plan for a Node with the **Components** that comprise the Node.
- **G1589**: Address issues in the appropriate governing **IPv6** transition plan as part of the Internet Protocol Version 6 (IPv6) Transition Plan for a Node.
- **G1590**: Include transition of all the impacted elements of the network as part of the **Internet Protocol Version 6** (IPv6) Transition Plan for a Node.
- **G1591**: Prepare **IPv6** Working Group products as part of the Internet Protocol Version 6 (IPv6) transition plan for a Node.
- **G1592**: Include interoperability testing in the plan as part of the **Internet Protocol Version 6** (IPv6) transition plan for a Node.
- **G1599**: Support both **Internet Protocol Version 4** (IPv4) and **Internet Protocol Version 6** (IPv6) simultaneously in the Node's **Domain Name System** (DNS) service.

Part 4: Node Guidance

- **G1600**: Obtain from DISA any and all **Internet Protocol Version 6** (IPv6) addresses used on DoD systems in the Node.

Best Practices

- **BP1705**: Design **DNS** infrastructure in accordance with appropriate governing **IPv6** Transition Office requirements.

P1141: Mobile Nodes

There have been significant advances in **Transmission Control Protocol/Internet Protocol** (TCP/IP) connectivity to mobile Nodes, such as airplanes, ships, and battlefield units; however, some significant challenges remain. In particular, it remains unclear to what extent mobile Nodes can directly utilize **Enterprise Services**, particularly the DISA **Core Enterprise Services** (CES). The characteristics of the link are likely to be extremely variable, including high frequency of topology changes, intermittent connectivity, higher than typical packet loss, low bandwidth, or high latency. Such characteristics are generally problematic for anything but the simplest of Enterprise Services. Components that use these Enterprise Services need to adapt in real-time to the presence or absence of the Enterprise Service and to the potentially intermittent performance of Enterprise Services. Consequently, the Component must be able to handle the failover and recover from Enterprise Service errors and gaps.

Managers of mobile Nodes that rely on the **Internet Protocol** (IP) for inter-Node communication should engage with the DISA **Net-Centric Enterprise Services** (NCES) program office to explore approaches for mobile use of the CES services. Alternatives might include development of specialized **Software Development Kits** (SDKs) that implement the required adaptive behavior or use of service **proxies** within the Node that could failover gracefully.

Many of the transport elements listed above may require extensions to account for the Node's intended mobile environment. For example, today's commercial routing protocols are not intended for the extent of dynamic and mobile behavior encountered in tactical military environments.

Another example is that **TCP** performance over satellite links is generally poor due to delays and blockages inherent to satellite links. TCP extensions and other transport protocols that have been developed to mitigate this risk should be considered for high bandwidth, high latency satellite communications.

Best Practices

- **BP1594**: Examine the use of **Transmission Control Protocol** (TCP) extensions and other transport protocols that have been designed to mitigate risk for high bandwidth, high latency satellite communications.

P1142: Domain Name System (DNS)

The **Domain Name System** (DNS) is a system that stores the relationships of host **Internet Protocol** (IP) address and their corresponding domain names in the equivalent of a distributed database (used here as a simplistic concept). The most important role of the DNS is to map IP addresses to human friendly domain names and back again. For example, where `nesi.spawar.navy.mil` may map to an **Internet Protocol Version 4** (IPv4) address of `128.49.49.225`, the **Internet Protocol Version 6** (IPv6) address might be `1080::34:0:417A`. For more information on DNS see [RFC 1034](#). DNS also performs other essential functions, such as reverse lookups (obtaining host names from IP addresses, which can be important for security) and email configuration (special DNS **Mail eXchange (MX) Records** indicate the **server** used to receive email for a host). These capabilities are fundamental to net-centric operations and are essential for other computing, network, and **Enterprise Services**.

The DNS namespace is hierarchical. At each level in the hierarchy, the namespace can be further divided into sub-namespaces called zones, which are delegated to other authoritative servers, and which can be further divided and delegated to other authoritative servers, and so on.

Each Node should implement DNS to manage hostname/address resolution within the Node, rather than use hard coded IP addresses, and use the DNS Mail eXchange (MX) Record capabilities to configure electronic mail delivery to the Node.

The DNS implementation should reflect the guidance provided in the *Domain Name System Security Technical Implementation Guide*. The **STIG** addresses implementation options such as the choice of basic DNS server types (primary, secondary, caching-only), use of a split-DNS design, location of servers in the network and relationship to other network entities, secure administration, security of zone transfers, and initial configuration.

Consider operational performance constraints, such as narrow bandwidth and intermittent connectivity, in the design of the Node's DNS. It may be desirable, for instance, to implement a caching-only DNS server for constrained environments.

Guidance

- [G1662](#): Follow the guidance provided in the **Security Technical Implementation Guide** (STIG) for **Domain Name System** (DNS) implementations.
- [G1595](#): Implement **Domain Name System** (DNS) to manage hostname/address resolution within the Node.
- [G1596](#): Use **Domain Name System** (DNS) **Mail eXchange (MX) Record** capabilities to configure electronic mail delivery to the Node.
- [G1598](#): Allow dynamic **Domain Name System** (DNS) updates to the Node's internal DNS service by local **Dynamic Host Configuration Protocol** (DHCP) **server(s)**.
- [G1599](#): Support both **Internet Protocol Version 4** (IPv4) and **Internet Protocol Version 6** (IPv6) simultaneously in the Node's **Domain Name System** (DNS) service.
- [G1600](#): Obtain from DISA any and all **Internet Protocol Version 6** (IPv6) addresses used on DoD systems in the Node.

Best Practices

- [BP1597](#): Consider operational performance constraints in the design of the Node's **Domain Name System** (DNS).
- [BP1663](#): Design a **Domain Name System** (DNS) in coordination with the appropriate governing Internet Protocol Version 6 (IPv6) Transformation Office.
- [BP1705](#): Design **DNS** infrastructure in accordance with appropriate governing **IPv6** Transition Office requirements.

P1143: Routers

Routers not only provide the main connection to the **Global Information Grid (GIG)**, but they also are a first line of **computer network defense**. These complex devices also provide security filtering, address management, network management, and time synchronization. A **GIG Router Working Group (GRWG)** is addressing implementation issues.

Components should be able to operate in a heterogeneous environment. The presence of **Internet Protocol Version 4 (IPv4)** and **Internet Protocol Version 6 (IPv6)** packets and services in a dual stack environment should not cause a degradation of application performance.

Routing capabilities in real-time, dynamic and mobile environments, such as at the tactical edge, are still in their infancy. Routing capabilities continue to be defined, prototyped and refined in a variety of working groups, such as the GRWG and Office of the Secretary of Defense **Joint Airborne Network (JAN) Working Group**.

Guidance

- **G1601**: Use configurable **routers** to provide dynamic **Internet Protocol (IP)** address management using **Dynamic Host Configuration Protocol (DHCP)**.
- **G1602**: Use configurable **routers** to provide static **Internet Protocol (IP)** addresses.
- **G1604**: Use configurable **routers** to provide time synchronization services using **Network Time Protocol (NTP)**.
- **G1605**: Use configurable **routers** to provide **multicast** addressing.
- **G1606**: Manage **routers** remotely from within the **Node**.
- **G1607**: Configure routers according to **National Security Agency (NSA)** [Router Security Configuration](#) guidance.

Best Practices

- **BP1699**: Configure **routers** in accordance with the Network **Security Technical Implementation Guide (STIG)**.
- **BP1700**: Configure **routers** in accordance with Enclave **Security Technical Implementation Guide (STIG)**.

P1144: Time Services

Net-centric operations and security depend on date and time synchronization. Many **protocols** rely upon synchronized time to function properly, particularly security protocols. Mission **Component** logic and the usefulness of data can also suffer if there is not a common understanding and synchronization of time across the **enterprise**.

Guidance

- **G1604**: Use configurable **routers** to provide time synchronization services using **Network Time Protocol** (NTP).
- **G1608**: Obtain the reference time for the Node time service from a globally synchronized time source.
- **G1609**: Arrange for a backup time source for the Node time service.

P1145: Mobile and Dynamic Networks

Nodes can be mobile or deployable as well as fixed. Mobile networks, by their very nature, are untethered and usually reliant upon Radio Frequency (RF) transmissions. The challenge to be addressed herein is that of ensuring uninterrupted **Global Information Grid** (GIG) interoperability as the underlying network changes dynamically.

Note: *A goal of mobile or deployable Nodes is that they can plug into different locations in the GIG without loss of interoperability.*

P1146: Multicast

Multicast addressing currently supports various groups throughout the **DoD** to provide capabilities such as **collaboration** and alerting; the use of multicast addressing is growing. Multicast capability is being actively engineered into the **Global Information Grid** (GIG). Careful planning is still required, however, until multicast becomes ubiquitous across the entire GIG.

Guidance

- **G1601**: Use configurable **routers** to provide dynamic **Internet Protocol** (IP) address management using **Dynamic Host Configuration Protocol** (DHCP).
- **G1610**: Configure the **Dynamic Host Configuration Protocol** (DHCP) services to assign **multicast** addresses.

Best Practices

- **BP1706**: Design node networks, including the selection of **Components** and configuration, to support **multicasting** even if not currently used.

P1147: Network Information Assurance

Implementation of the DoD **Information Assurance** (IA) Strategic Plan is required to comply with the DoD **Net-Ready Key Performance Parameter** (NR-KPP). Components that implement IA, however, can be a barrier to interoperability by default; proper implementation is critical. Furthermore, as net-centric applications and services emerge, so too will the need to dynamically configure the IA Components to permit net-centric operations. As an example, **access control** based on **Internet Protocol** (IP) address would not work, as the addresses of service users will not be known a priori when such services are dynamically discoverable.

The DoD provides requirements and extensive guidance for the implementation of information assurance at the [DISA Information Assurance Support Environment \(IASE\)](#) Web site. In particular, the Network **Security Technical Implementation Guide** (STIG) on the IASE Web site provides guidance for the network implementation, particularly the boundary between the Node's internal network and external networks. It identifies several IA systems, capabilities, and configurations as listed below and provides guidance for implementation of each.

Rather than repeating the contents of specific guidance in this document, readers should check the IASE Web site for current Network IA guidance on topics such as the following:

- External Network **Intrusion Detection System** (IDS), anomaly detection, or prevention device if required by the **Computer Network Defense Service Provider** (CNDSP)
- **Router** Security with **Access Control Lists**
- **Firewall** and application level **proxies** (may be separate device to proxy applications)
- Internal **Network Intrusion Detection** (NID) system
- DMZ, if applicable for publicly accessible services
- Split Domain Name Service (DNS) architecture
- Secure devices and operating systems (i.e., **STIG** compliant)
- Ports and **protocols**

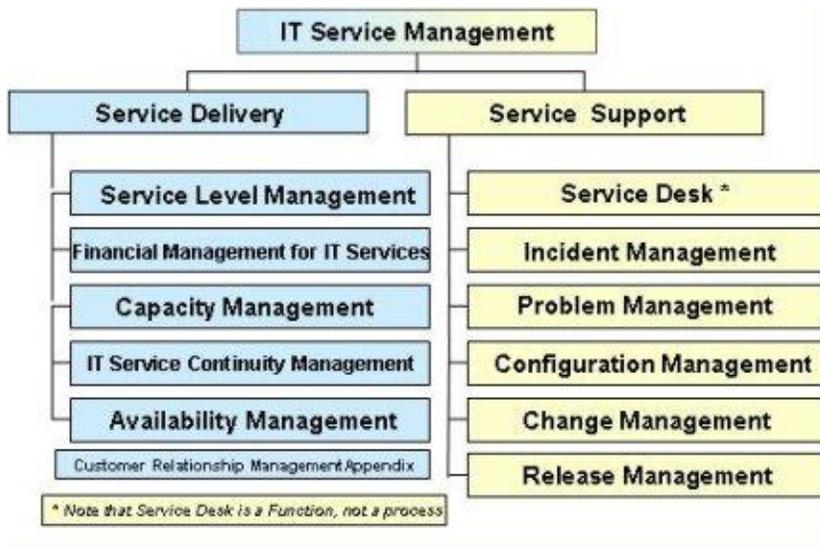
Furthermore, DoD **computer network defense** (CND) policies *mandate all owners of DoD information systems and computer networks enter into a service relationship with a CNDSP provider.*

Best Practices

- **BP1701**: Configure **Components** for **Information Assurance** (IA) in accordance with the Network **Security Technical Implementation Guide** (STIG).

P1148: Enterprise Management Services

Enterprise Management Services (EMS) are fundamental to execution of **Service Level Agreements** (SLAs), which are inherent in net-centric operations. EMS services are often used internal to a Node using a variety of **commercial off-the-shelf** (COTS) tools. In a net-centric context, though, EMS must be extended to address inter-nodal service availability and reliability guarantees. Beyond the simpler task of maintaining status information such as link status or service up/down status, EMS must be extended to address complex service arrangement that may involve multiple, orchestrated services. Additionally, coordinated help-desk and reporting will be needed. Some of these topics are being addressed under the DoD **NetOps** concept.



11181

P1149: Virtual Private Networks (VPN)

Virtual Private Networks (VPNs) create a private "tunnel" within a network by encrypting traffic between specified end points. If a VPN is required at a Node, it should be implemented in accordance with the guidance provided in the Network **STIG**. Services and information intended to be broadly accessible to other **Global Information Grid** (GIG) Nodes should not be placed behind a VPN because it will be reachable to only the Nodes that are part of the VPN.

Guidance

- [G1667](#): Implement **Virtual Private Networks** (VPNs) in accordance with the guidance provided in the Network **Security Technical Implementation Guide** (STIG).

Best Practices

- [BP1702](#): Do not place services and information intended to be broadly accessible to other nodes behind a **Virtual Private Network** (VPN).

P1150: Trusted Guards

Trusted guards are accredited to pass information between two networks at different security levels, such as between **SECRET General Service (GENSER)** and **TOP SECRET Sensitive Compartmented Information (TS SCI)** level networks, according to well defined rules and other controls. Guard products only pass defined types of information (e.g., email, images, or formatted messages). A key challenge is how to implement net-centric operations across trusted guards in the presence of **CES** services. See the [Cross-Domain Interoperation](#) perspective for additional information.

Best Practices

- [BP1653](#): Do not build dedicated Node guard products.
- [BP1654](#): Do not build dedicated **Component** guard products.
- [BP1668](#): Acquire and configure approved guard products with the help of the Government program offices that acquire such guards.
- [BP1669](#): Select **XML**-capable **trusted guards**.

P1151: Integration of Non-IP Transports

Systems that are not **Internet Protocol** (IP) networked, such as aircraft data links (**Link-16, SADL**, etc.), should implement IP gateways to interoperate with the **Global Information Grid** (GIG) until IP is supported natively. Most such systems already have plans for transition to IP networking, and gateways are an interim measure.

Implement these gateways as **services** in accordance with **NESI Part 5: Developer Guidance**. This does not mean that the service would be limited to request/reply or other such usage patterns. In fact, for high-frequency data, such as track reporting, a function of the service could be to set up an out-of-band communication with a subscriber.

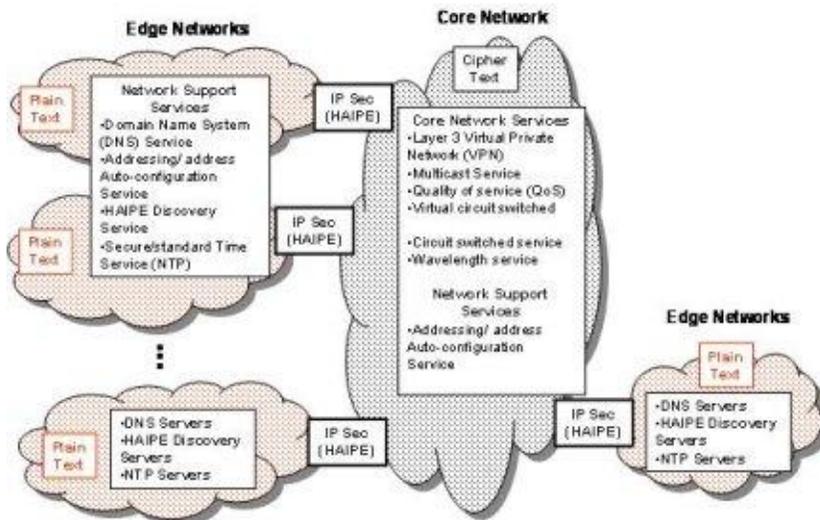
Guidance

- **G1611**: Implement Internet Protocol (**IP**) gateways to interoperate with the **Global Information Grid** (GIG) until IP is supported natively for **Components** that are not IP networked, such as aircraft data links (**Link-16, SADL**, etc.).
- **G1612**: Implement Internet Protocol (**IP**) gateways as a **service**.

P1152: Black Core

The DoD will be aggregating **Internet Protocol (IP)** packet traffic from multiple security enclaves onto network segments secured at the network layer in the protocol stacks; these segments, called the Black Core, are enabled through the use of **High Assurance Internet Protocol Encryption (HAiPE)** devices. Challenges to the implementation of HAiPE devices and the Black Core include organic support for the following: IP-based **quality of service (QoS)**, dynamic unicast IP routing, support for dynamic **multicast IP** routing, support for mobility, and support for simultaneous **Internet Protocol Version 6 (IPv6)** and **Internet Protocol Version 4 (IPv4)** operation.

The Black Core is a concept fundamental to **Global Information Grid (GIG)** networking, but actionable guidance is still in its infancy. Interoperability with the Black Core will require active monitoring by the Node's management and program offices. The basic architecture of the Black Core is shown below. The Node typically provides one or more edge networks as shown in the diagram, along with the services indicated. The edge (Node) networks are sometimes referred to as **Plain Text (PT)** networks, while the Black Core is the **Cipher Text (CT)** network.



I1182

Best Practices

- **BP1670:** Monitor Black Core implementation issues and prepare a plan for local implementation in coordination with system programs fielded within the Node.
- **BP1671:** Consider Black Core transition whenever there is a significant Node network design or configuration decision to make in an effort to avoid costly downstream changes caused by Black Core transition.

P1153: Node Computing Infrastructure

Several elements of the computing infrastructure have a significant effect on **Global Information Grid** (GIG) interoperability. Other elements of the computing infrastructure, such as Host Management, Backup/Restore, and Software/Patch Distribution are outside the scope of NESI because they have little impact on net-centricity or interoperability across GIG Nodes. The following elements have a direct bearing on net-centricity or interoperability:

- [Web Client Platform](#)
- [Web Application Infrastructure](#)
- [Host Information Assurance](#)
- [Domain Directories](#)
- [Instrumentation and Metrics](#)

P1154: Web Client Platform

Web clients (both desktops and **servers**) should be capable of accessing **Java Platform, Enterprise Edition** (Java EE) **services** and **.NET** services; service developers are free to choose the best technology for their service.

Two key elements of the standard frameworks follow:

- [Browser](#)
- [Common Access Card \(CAC\) Reader](#)

Guidance

- [G1613](#): Prepare a **Node** to host new **Component** services developed by other Nodes or by the **enterprise** itself.

Best Practices

- [BP1614](#): Prepare a **Node** for the possibility of becoming a new **Component** service within another Node.
- [BP1672](#): Be prepared to integrate fully with the **Information Assurance** (IA) infrastructure.
- [BP1673](#): Be prepared to integrate fully with the **Enterprise Management Services** (EMS) infrastructure.

P1155: Browser

Web browsers are fundamental to the DoD vision of net-centric information sharing and access to distributed **services**. Because **Global Information Grid** (GIG) interoperability partners may not be known a priori, Web browsers should support a wide breadth of browser technologies, such as **JavaScript**, Java **applets**, and **plug-ins**.

The browser should be configured in accordance with the Web Server Security Technical Implementation Guide (**STIG**), Desktop Applications STIG, and Windows 2003/XP/2000 Addendum STIG.

Best Practices

- **BP1674**: Configure the **browser** in accordance with the Web Server Security Technical Implementation Guide (**STIG**), Desktop Applications STIG, and Windows 2003/XP/2000 Addendum STIG.
- **BP1615**: Select **Web browsers** that support a wide breadth of current browser extension technologies.

P1156: Common Access Card (CAC) Reader

Smart Cards provide greatly increased security for multiple applications. The usefulness of a smart card is based on its intrinsic portability and security. A typical smart card has the same dimensions as a standard credit card and appears to be very similar with the exception of a set of gold contacts. When inserted into a reader, these contacts provide power to a microprocessor located on the smart card; the smart card is thus able to store and process information, in particular cryptographic keys and algorithms for providing digital signatures and for use with other encryption. A major impediment to the widespread use of smart cards has been interoperability. Unfortunately, smart cards are currently not vendor interoperable and therefore must use specific software and smart card readers. This is an issue that is being addressed by the **National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL)**.

Guidance

- [G1619](#): Configure **clients** with a **Common Access Card (CAC)** reader.

P1157: Web Infrastructure

A Web infrastructure allows software developers to deploy Web-enabled applications, **services** and other software in a Node. While many Web infrastructures exist, most software will converge on one or two popular platforms or technologies (e.g., Apache; **Java Platform, Enterprise Edition**; **.NET**; etc.). The Node should provide common shared Web infrastructures for software deployments to minimize unnecessary duplication of these common environments. A common Web infrastructure will also allow Nodes to better provide full integration with local **Information Assurance** (IA) and **Enterprise Management Services** (EMS) infrastructures as well as **CES** and **COI services** available both internally and externally to the Node.

There are three major elements to Web infrastructure that need to be addressed at the Node:

- [Web Portal](#)
- [Web Server](#)
- [Web Application Containers](#)

Guidance

- [G1621](#): Provide a Node Web infrastructure for all **Components** within the Node.

Best Practices

- [BP1675](#): In the Node's Web infrastructure, support the technologies and standards used by the **CES** services under development as well as any technologies and standards used for **Community of Interest** (COI) services.
- [BP1677](#): Consider using Web **proxy** servers and load balancers.
- [BP1707](#): Configure and locate elements of the Node Web infrastructure in accordance with the Web Server **Security Technical Implementation Guide** (STIG).
- [BP1708](#): Configure and locate elements of the Node Web infrastructure in accordance with the Desktop Applications **Security Technical Implementation Guide** (STIG).
- [BP1709](#): Configure and locate elements of the Node Web infrastructure in accordance with the Network **Security Technical Implementation Guide** (STIG).

P1158: Web Portal

A Web portal provides an environment for hosting small Web applications called **portlets**, and allows for content selection, arrangement and other visual preferences tailored to each user. Though not strictly essential for **Global Information Grid** (GIG) interoperability, it is reasonable that some GIG net-centric services and applications will provide portal-based Web applications that Nodes may want to host locally. To reduce issues of portability, Web portals provided by the Node should support widely accepted standards such as **JSR-168** and **Web Services for Remote Portlets** (WSRP). However, because commercial products also provide non-portable proprietary interfaces, there is a risk that multiple Web portal products may be required or that the portlet would have to be reengineered to work on an existing Node portal.

Note: See the **Web Portals** perspective [P1077] in NESI Part 5: Developer Guidance for additional information.

Best Practices

- **BP1710:** Support appropriate and widely accepted standards for Web portals provided by the Node.

P1159: Web Server

Web server technology is becoming fundamental in making information visible and accessible to external **Global Information Grid** (GIG) users. The most significant barrier to interoperation is security. Making information accessible to a community of users as large as the GIG necessitates the implementation of **authentication** and **authorization** technology that is sufficient to prove a user's identity and that is scalable, respectively. Web servers should provide DoD **Public Key Infrastructure** (PKI) based authentication and role based authorization mapped to **certificate** attributes as described in the applicable **Security Technical Implementation Guides** (STIGs). Eventually, the container should integrate with the **Net-Centric Enterprise Services** (NCES) Security Service, when available. In the interim, authorization should be based on the **Electronic Data Interchange # Personnel Identifier** (EDI-PI) contained in the PKI certificate attributes. The use of the EDI-PI as the attribute on which to base authorization decisions is a matter of debate and ongoing engineering, as there are issues about the issuance of EDI-PI to certain user populations, such as coalition users. In the absence of an EDI-PI attribute, other attributes should be used for authorization decisions.

Note: *For additional technical level guidance on Web servers, see NESI Part 5: Developer Guidance.*

P1160: Web Application Containers

Web application containers provide an environment for serving full, interactive application functionality and services on the **Web**. There are two major container technologies: **Java Platform, Enterprise Edition** (Java EE) and **.NET, NESI** expresses no preference regarding which of the two technologies is used; *NESI Part 5: Developer Guidance* addresses both (see, for example, **Java EE Environment** [P1037] and **Web Services with .NET** [P1079]).

The design and implementation of a Node's Web infrastructure should accommodate both Java EE and .NET. The rationale for this is that Nodes will likely have to host services locally and applications that were developed externally using either technology. Use Web services (**Simple Object Access Protocol** or SOAP, **XML**, etc.) to interoperate between Java EE and .NET applications or services. Such interoperation may be required, for example, when orchestrating Web services across Nodes as part of a Joint mission thread.

As is the case with Web servers, application containers should provide DoD **Public Key Infrastructure** (PKI) based authentication and role based **authorization** mapped to **certificate** attributes as described in the applicable STIGs. Eventually, the container should integrate with the **Net-Centric Enterprise Services** (NCES) Security Service when available. In the interim, base authorization on the **Electronic Data Interchange # Personnel Identifier** (EDI-PI) contained in the PKI certificate attributes. The use of the EDI-PI as the attribute on which to base authorization decisions is a matter of debate and ongoing engineering, as there are issues about the issuance of EDI-PI to certain user populations, such as coalition users. In the absence of an EDI-PI attribute, use other attributes for authorization decisions.

The Web application container should be capable of processing Web services protocols in accordance with the **Web Services Interoperability** (WS-I) Basic Profile. The container should also support XML security protocols including XML Encryption, XML Signature, and XML Key Management. These protocols are used in protecting content within an XML document that may be passed among multiple **orchestrated** Web services.

P1161: Host Information Assurance

Host **Information Assurance** (IA) protections are part of the DoD Information Assurance Strategic Plan, which in turn is a part of the **Net-Ready Key Performance Parameter** (NR-KPP) that gets assessed during the **Joint Capabilities Integration and Development System** (JCIDS) acquisition process. Failure to implement host information assurance protections could jeopardize the approval for a Node to operate on the **Global Information Grid** (GIG).

Guidance

- **G1622**: Implement **commercial off-the-shelf** (COTS) software that protects against malicious code on each operating system in the Node in accordance with the Desktop Application **Security Technical Implementation Guide** (STIG).
- **G1623**: Implement personal **firewall** software on **client** or **server** hardware used for remote connectivity in accordance with the Desktop Applications, Network and Enclave **Security Technical Implementation Guides** (STIGs).
- **G1624**: Install anti-**spyware** on all **client** and **server** hardware.

P1162: Domain Directories

Within and across Nodes, directory technologies such as Microsoft **Active Directory** (AD) or OpenLDAP are tools for system, network, and security administration. Many options exist on how Nodes employ these tools; however, interoperability issues can arise between **Global Information Grid** (GIG) Nodes if sub-enterprises employ these tools differently (even within the same technology family, such as AD).

Guidance on Active Directory implementation is being formed by the **DoD Active Directory Interoperability Working Group (DADIWG)**.

Implement Active Directory (AD), if used, in accordance with the recommendations of the DADIWG; also, periodically monitor the [DADIWG Web site](#) (user authorization required) for the status of GIG implementation issues.

Best Practices

- **BP1679**: Implement a Node that uses **Active Directory** (AD) in accordance with the recommendations of the DoD Active Directory Interoperability Working Group (DADIWG).

P1163: Instrumentation for Metrics

Performance has an impact on net-centric operations. Instrumentation is a term frequently used in association with the generation, collection, and analysis of performance metrics. In a dynamic environment, where **services** and information exchange partners may be dynamic, metrics can be a key factor in the selection of services. Performance metrics that are advertised externally and frequently updated allow potential service users the ability to select an implementation that meets their performance requirements, such as a measurement of reliability. Metrics are normally also needed to ensure performance is provided according to more traditional **Service Level Agreements** (SLAs), and for operations management.

Component services that are exposed to the **Global Information Grid** (GIG) by a Node should be instrumented to collect performance metrics. Metrics should be visible and accessible as part of the Component service registration and updated periodically. Standards for metrics are not defined but are expected at some point in the future by appropriate GIG working groups.

Some sample metrics that may be appropriate for **Web services** are in the following table:

SLA Metric	Metric Description
Availability	How often is the service available for consumption?
Accessibility	How capable is the service of serving a client request now?
Performance	How long does it take for the service to respond?
Compliance	How fully does the service comply with stated standards?
Security	How safe and secure is it to interact with this service?
Energy Efficiency	How energy-efficient is this service for mobile applications?
Reliability	How often does the service fail to maintain its overall service quality?

Best Practices

- **BP1680**: Instrument **Component** services that a Node exposes to the **Global Information Grid** (GIG) to collect performance metrics.
- **BP1681**: Make **Component** services metrics visible and accessible as part of the service registration and updated periodically.
- **BP1867**: Use metrics to track responsiveness to user information sharing needs.

P1164: Node Application Enterprise Services

The DoD has developed an **Enterprise Services Strategy** that obligates Nodes to employ **Enterprise Services** to achieve net-centric information sharing. The ultimate goal is to connect people or systems that need information with people or systems that have the needed information. In the strategy, information is considered to be data and/or services. The connection between the information providers and information consumers is through the use of core **enterprise** capabilities. Within the DoD, DISA is chartered to define and develop these capabilities through a project called **Net-Centric Enterprise Services** (NCES). NCES has the following vision:

NCES will enable the secure, agile, robust, dependable, interoperable data-sharing environment for DoD where warfighter, business, and intelligence users share knowledge on a global network that facilitates information superiority, and accelerates decision-making, effective operations, and net-centric transformation.

In order to accomplish this interconnectivity, NCES has identified nine capabilities that are mapped to services. Collectively, these services are called the **Core Enterprise Services** (CESs).



11183

Discovery	Search, locate or publish data (content), other capabilities (services), or users across the Global Information Grid (GIG)
IA/Security	Authorizes and authenticates Global Information Grid (GIG) users to ensure the confidentiality and integrity of information and services
Mediation	Translates, brokers, aggregates, fuses or integrates data into commonly understood formats
Messaging	Distributed, machine-to-machine messaging for notifications and alerts
Enterprise Service Management	Monitor/manage Global Information Grid (GIG) Enterprise Services against operational performance parameters to ensure reliability and availability of critical capabilities
Collaboration	Allows users to work together securely on the network by way of video, audio, text chat, white boarding, online meetings, work groups, application sharing

Part 4: Node Guidance

User Assistance	Provides automated "helper" capabilities and user preferences to help maximize user efficiency in task performance
Storage	Provides physical and virtual places to host and retain data for purposes such as content staging, continuity of operations, or archival
Application	Provides the resources necessary to provision, operate and maintain Net-Centric Enterprise Services (NCES) capabilities

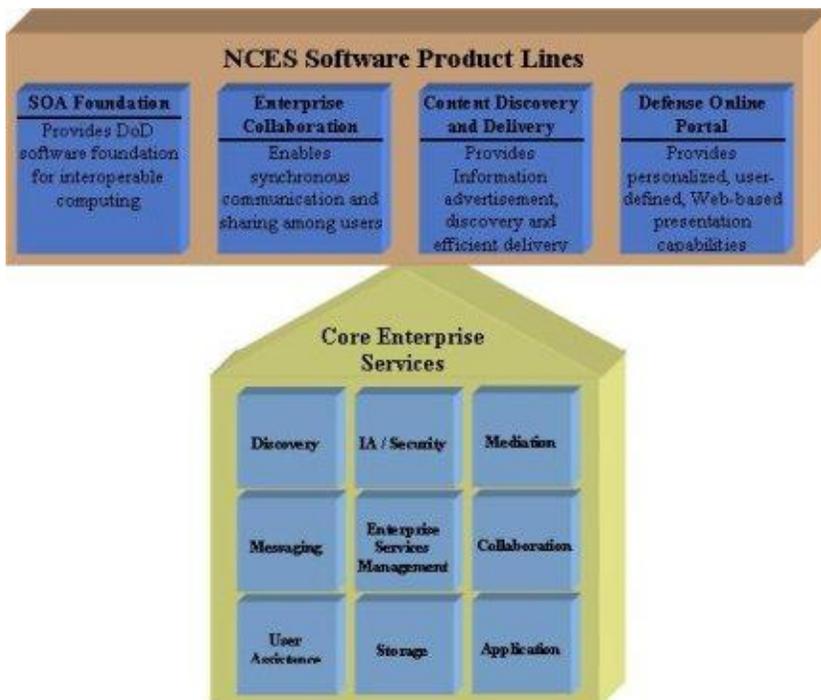
The nine CES are being developed for the entire GIG enterprise by NCES. NCES is using a **Software Product Line** (SPL) approach to facilitate the building of the CES. The Software Engineering Institute (SEI) defines SPL as follows:

A software product line (SPL) is a set of software-intensive systems that share a common, managed set of features satisfying the specific needs of a particular market segment or mission and that are developed from a common set of core assets in a prescribed way. (Source: [Software Engineering Institute](#))

NCES has divided the problem into four product lines:

SOA Foundation	Provides the DoD software foundation for interoperable computing
Enterprise Collaboration	Enables synchronous communication and sharing among users
Content Discovery and Delivery	Provides Information advertisement, discovery and efficient delivery
Defense Online Portal	Provides personalized, user-defined, Web-based presentation capabilities

DISA will provision the CES services to operate on the **Unclassified but Sensitive Internet Protocol Router Network (NIPRNet)** and **Secret Internet Protocol Router Network (SIPRNET)** global networks, initially operating from DISA **Defense Enterprise Computing Centers (DECCs)**.



11184

Part 4: Node Guidance

The CES and SPL approach is very flexible. As a consequence, the exact mechanism of how CES services are employed by Nodes is a topic of active discussions.

Detailed Perspectives

- [Overarching Issues](#)
- [Core Enterprise Services \(CES\)](#)

P1165: Overarching Issues

Overarching Node Application Enterprise Services issues include maturity, availability, disconnected operations, cross-domain security, and compliance. These elements equate to the following perspectives:

- Maturity: [CES Definitions and Status](#)
- Availability: [CES Parallel Development](#)
- Disconnected operations: [CES and Intermittent Availability](#)
- Cross-domain security: [Cross-Domain Interoperation](#)
- Compliance: [Net-Ready Key Performance Parameter \(NR-KPP\)](#)

Part 4: Node Guidance

Machine-to-Machine Messaging	Provides reliable machine-to-machine message exchange across the enterprise
Metadata Services	Provides access to Extensible Markup Language (XML) data elements, taxonomy galleries, schemas, and validation and generation tools for DOD software developers
DoD Web Services Profile	Provides specifications and implementation guidelines to maximize interoperability across DOD Web service implementations

NCES Increments will be rolled out every 24-26 months. Consider the NCES increment schedule in scheduling Node evolution in coordination with systems within the Node.

Guidance

- **G1576**: Provide an environment to support the development, build, integration, and test of net-centric capabilities.
- **G1626**: Identify which **Core Enterprise Services** (CES) capabilities the Node **Components** require.
- **G1627**: Identify the priority of each **Core Enterprise Services** (CES) capability the Node **Components** require.
- **G1629**: Identify which **Net-Centric Enterprise Services** (NCES) capabilities the Node requires during deployment.

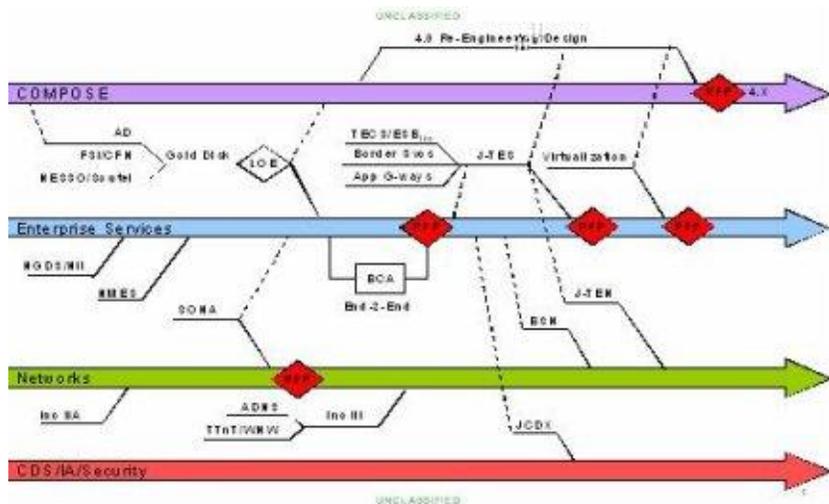
Best Practices

- **BP1661**: Engage with the **Net-Centric Enterprise Services** (NCES) program office to explore approaches for mobile use of the **Core Enterprise Services** (CES) services in mobile Nodes that rely on **Transmission Control Protocol/Internet Protocol** (TCP/IP) for inter-node communication.
- **BP1675**: In the Node's Web infrastructure, support the technologies and standards used by the **CES** services under development as well as any technologies and standards used for **Community of Interest** (COI) services.
- **BP1683**: Coordinate the Node schedule with the **Net-Centric Enterprise Services** (NCES) schedule.
- **BP1684**: Coordinate the Node schedule with the **Component** schedules.

Examples

The following is an example of how a **Service-Oriented Architecture** (SOA) Roadmap could be developed by the Navy PEO C4I & Space Networks, IA and Enterprise Services Program Management Office (PMW160) for a project called COMPOSE. The Roadmap lays out the deliveries for four layers: COMPOSE itself, **Enterprise Services**, Networks, and Security. The milestones and the availability and interdependences of the various parts are documented.

Part 4: Node Guidance



I1186

P1167: CES Parallel Development

Availability of the **Core Enterprise Services** (CES) will be a continuing challenge until all services reach full maturity and operational status. The following table is taken from the **Net-Centric Enterprise Services** (NCEs) workspace of the **Defense Online** Web site and shows the availability of services comprising the NCEs **Discovery** capability. Designating a CES liaison should help to monitor the availability of CES functionality and report on them back through the engineering processes of the Node and **Components** within the Node. Conversely, the engineering processes for the Node and Components should specifically include provisions for incremental implementation of the CES services.

To accelerate the maturation and implementation of the CES, DISA established an **Early Adopter** process. Early adopters can participate in service pilots, as described in the *NCEs Pilot Participants Guide*.

Use the early adopter process and service pilots to accelerate implementation of the CES within the Node. Many factors influence the decision to participate in the early adopter process and pilots including acquisition phase, funding, mission, and priorities for individual systems as well as the aggregate Node. Develop a Node-specific service implementation plan.

Nodes operating at special classification levels should coordinate with other Nodes within the same level and with DISA to host CES services on the relevant networks.

Guidance

- **G1577**: Maintain an **Enterprise Service** schedule for interim and final **enterprise** capabilities within the Node.
- **G1578**: Define a schedule for **Components** that includes the use of the **Enterprise Services** defined within the Node's enterprise service schedule.
- **G1627**: Identify the priority of each **Core Enterprise Services** (CES) capability the Node **Components** require.

Best Practices

- **BP1683**: Coordinate the Node schedule with the **Net-Centric Enterprise Services** (NCEs) schedule.
- **BP1684**: Coordinate the Node schedule with the **Component** schedules.
- **BP1694**: Coordinate with other Nodes having the same compartmentalization needs and with **DISA** to host compartmentalization CES.
- **BP1695**: Designate a **CES** liaison to monitor the availability of services.
- **BP1696**: Use the Early Adopter process and service pilots to accelerate implementation of the **CES** services within the Node.
- **BP1697**: Make the parallel development of **CES** outside the control of the Node a part of the Node's risk management activities.
- **BP1649**: Specifically include provisions for incremental implementation of the **CES** services.
- **BP1650**: Specifically include provisions for incremental implementation of the hosting Node's **CES** services for Node **Components**.

P1168: CES and Intermittent Availability

There are two related challenges: how to handle lapses in the availability of **Core Enterprise Services** (CES) and how to align inter-Node and intra-Node solutions. CES services may be unavailable for several reasons, including loss of connectivity, actual service unavailability, or service rejection. The lack of availability of CES services must not disrupt intra-node availability of locally hosted services. While alignment of intra- and inter-node technical solutions is very desirable, the interface to locally hosted **Components** must not be dependent on the availability of CES services.

Specific guidance is largely dependent upon the specific Node operating environment and mission. There appear to be some basic options for meeting these challenges:

- Locally host failover copies of certain CES services. Components that are dependent upon **Enterprise Services** for infrastructure functions, such as security, continue to operate after failing over to the local instances until **enterprise** accessibility is re-established. This approach requires replication of enterprise services data (the data used by the enterprise services) between the local failover services and the "master" enterprise services. It also requires development of failover behavior in the applications, services, and infrastructure.
- Develop Components to be adaptive, applying default rules and behaviors when Enterprise Services are inaccessible. This approach, along with the definition of the default rules and behaviors would depend on factors such as the sensitivity and importance of the information involved. For example, access control decisions might default to local capabilities such as **Active Directory** local user accounts. Or local caching might be used to retain the most recently known values for information such as previously discovered services.
- Employ separate external-facing and internal-facing implementations of published services so that external disruptions do not affect local accessibility. The external-facing copy of the service could use Enterprise Services, and the internal-facing copy could implement local Node behavior. As an example, the external-facing copy could implement **Public Key Infrastructure** (PKI) **authentication** and **authorization**, whereas the internal-facing copy could implement Active Directory security. The challenge in this approach is in the coordination of the external-facing and internal-facing copies of such services, such as to provide shared access to databases or replication of data between the external-facing and internal-facing implementations.

Nodes and Components will likely employ some combination of, or evolution of, the above options.

Uniformity and alignment between the technical mechanisms for accessing local services and Enterprise Services should be an objective. Where possible, the burden of providing such uniformity and alignment should rest on the Node infrastructure, rather than the individual Components within the Node, thus isolating the complexities and making them more manageable. Consider the necessity of using CES-provided SDKs and **Key Interface Profile** (KIP) compliance when formulating an approach; use of an approved SDK may drive separation of external-facing and internal-facing implementation described in the last option above. Finally, the immaturity of the CES services and the alignment of local and external services access, as a whole, should figure prominently in the risk management activities of the Node and Components within the Node.

Guidance

- **G1630**: Comply with the applicable **Global Information Grid** (GIG) **Key Interface Profiles** (KIPs) for implemented **Core Enterprise Services** (CES) in the Node.
- **G1631**: Expose **Core Enterprise Services** (CES) that comply with the applicable **Global Information Grid** (GIG) **Key Interface Profiles** (KIPs) in all Node services **proxies**.

Best Practices

- **BP1651**: Do not implement **server** side **CES** functionality for **Components**.

P1169: Cross-Domain Interoperation

By and large, the implementation of net-centric concepts across security domains has not been defined. Trusted guards do not act as network **routers**; information to be transferred across a guard is delivered to the guard, processed, and then delivered to a defined endpoint on the other side if the rules are satisfied. The guard in the middle disrupts the normal pattern for use of the **CES** services.

In order for **services** to work through the trusted guards that interconnect different domains, there must be a well defined set of messages that can be passed through the guard to effect the conversation necessary to use the service and return results. This restriction, if built into the service's interface, could be unduly restrictive on the design of the interface.

It may be more practical for each such service to provide service proxies for use in the other security domains, and corresponding client proxies in the local domain. The server **proxy** and client proxy for the service might then communicate across the trusted guard in a private, high efficiency manner that the guard can process. But even this approach is restrictive in that the server proxies have to be installed in the other security domains, and this departs from some fundamentals of net-centric concepts such as dynamic **service discovery**.

Until such approaches are prototyped and explored more fully, Nodes should anticipate that services will not be capable of cross-domain invocation. Furthermore, for services that have utility in other security domains, implementer should consider providing copies of such services for hosting in the other domains, and use **XML** document transfers across the trusted guard to keep the copies in synchronization. This approach depends on many factors, and may not be suitable for all services.

Guidance

- [G1613](#): Prepare a **Node** to host new **Component** services developed by other Nodes or by the **enterprise** itself.

Best Practices

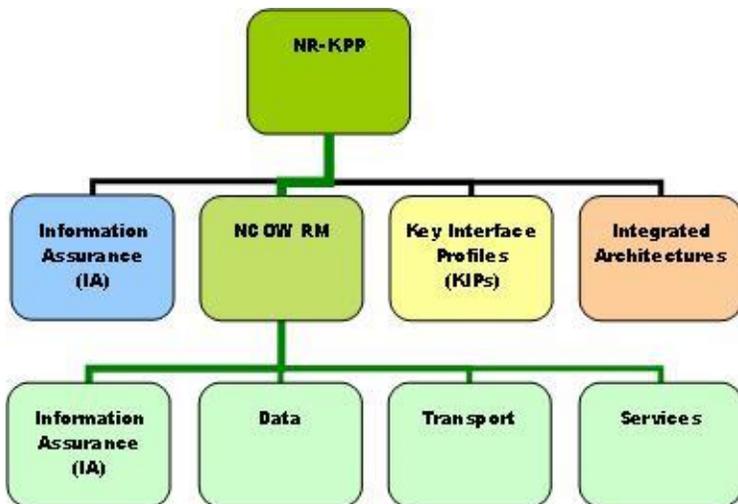
- [BP1691](#): Use **Node** implemented **Service Discovery (SD)** to meet compartmentalization needs.
- [BP1698](#): Plan for the event that **Component** services within a **Node** cannot be invoked across security domains.
- [BP1614](#): Prepare a **Node** for the possibility of becoming a new **Component** service within another Node.

P1170: Net-Ready Key Performance Parameter (NR-KPP)

The following information is from the **Defense Acquisition University** (DAU) [Defense Acquisition Guidebook, Chapter 7.3.4](#). The **Net-Ready Key Performance Parameter** (NR-KPP) has been developed to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP, and incorporates net-centric concepts for achieving **Information Technology** (IT) and **National Security Systems** (NSS) interoperability and supportability. The NR-KPP assists Program Managers, the test community, and Milestone Decision Authorities in assessing and evaluating IT and NSS interoperability.

The NR-KPP assesses information needs, information timeliness, **information assurance**, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. Program managers will use the NR-KPP documented in **Capability Development Documents** (CDD) and **Capability Production Documents** (CPD) to analyze, identify, and describe IT and NSS interoperability needs in the **Information Support Plan** (ISP) and in the test strategies in the Test and Evaluation Master Plan.

The following diagram explains the relationships of the **Global Information Grid** (GIG) **Key Interface Profiles** (KIPs), **Net-Centric Operations and Warfare Reference Model** (NCOW RM), **ASD(NII)** Net-Centric Checklist [\[R1177\]](#), and the Net-Ready Key Performance Parameter (NR-KPP) [\[R1176\]](#).



11187

Detailed Perspectives

- [Information Assurance \(IA\)](#)
- [Net-Centric Operations and Warfare Reference Model \(NCOW RM\)](#)
- [Key Interface Profile \(KIP\)](#)
- [Integrated Architectures](#)

P1171: Information Assurance (IA)

Most Nodes, when delivering a capability to the warfighter or business domains, will use **Information Technology** (IT) to enable or deliver that capability. For those Nodes, developing a comprehensive and effective approach to **IA** is a fundamental requirement and is key in successfully achieving Node's objectives. The DoD defines IA as follows [see [DoDD 8500.1](#), Enclosure 2 Definitions (E2.1.17)]:

Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

DoD policy and implementing instructions on information assurance are in the 8500 series of DoD publications. Nodes and **Components** for programs should be familiar with statutory and regulatory requirements governing information assurance and understand the major tasks involved in developing an IA organization, defining IA requirements, incorporating IA in the Node's and Component architecture, developing an acquisition IA strategy (when required), conducting appropriate IA testing, and achieving IA certification and accreditation for the program.

Guidance

- **G1632:** Certify and accredit Nodes with all applicable DoD **Information Assurance** (IA) processes.
- **G1633:** Host only DoD **Information Assurance** (IA) certified and accredited **Components**.
- **G1634:** Certify and accredit **Components** with all applicable DoD **Information Assurance** (IA) processes.

P1172: Net-Centric Operations and Warfare Reference Model (NCOW RM)

The **Net-Centric Operations and Warfare Reference Model** (NCOW RM) represents the strategies for transforming the **enterprise** information environment of the Department. It is an architecture-based description of activities, services, technologies, and concepts that enable a net-centric enterprise information environment for warfighting, business, and management operations throughout the Department of Defense. Included in this description are the activities and services required to establish, use, operate, and manage this net-centric enterprise information environment. Major activity blocks include the generic user-interface (A1), the intelligent-assistant capabilities (A2), the net-centric service (core, **Community of Interest**, and enterprise control) capabilities (A3), the dynamically allocated communications, computing, and **storage** media resources (A4), and the enterprise information environment management components (A5). Also included is a description of a selected set of key standards and/or emerging technologies that will be needed as the NCOW capabilities of the **Global Information Grid** (GIG) are realized.

Transforming to a net-centric environment requires achieving four key attributes: reach, richness, agility, and assurance. The initial elements for achieving these attributes include the **Net-Centric Enterprise Services** (NCES) Strategy, the **DoD Net-Centric Data Strategy**, and the DoD **Information Assurance** (IA) Strategy to share information and capabilities. The NCOW RM incorporates (or will incorporate) these strategies as well as any net-centric results produced by the Department's **Horizontal Fusion** (HF) pilot portfolio.

The NCOW RM provides the means and mechanisms for acquisition program managers to describe their transition from the current environment (described in **GIG Architecture Version 1**) to the future environment (described in **GIG Architecture Version 2**). In addition, the NCOW RM will be a key tool during program oversight reviews for examining integrated architectures to determine the degree of net-centricity a program possesses and the degree to which a program can evolve to increased net-centricity. Compliance with the NCOW RM is one of the four elements that comprise the **Net-Ready Key Performance Parameter** (NR-KPP).

Guidance

- **G1636**: Comply with the **Net-Centric Operations and Warfare Reference Model** (NCOW RM).

P1173: Key Interface Profile (KIP)

The following information is from the **Defense Acquisition University** (DAU) [Defense Acquisition Guidebook, Chapter 7.3.4.2](#). A **Key Interface Profile** (KIP) is the set of documentation produced as a result of interface analysis which designates an interface as key; analyzes it to understand its architectural, interoperability, test and configuration management characteristics; and documents those characteristics in conjunction with solution sets for issues identified during the analysis. The profile consists of refined operational and systems view products, Interface Control Document/Specifications, Systems Engineering Plan, Configuration Management Plan, **Technical Standards View** (TV-1) with SV-TV Bridge, and procedures for standards conformance and interoperability testing. Relevant **Global Information Grid** (GIG) KIPs, for a given capability, are documented in the **Capability Development Document** and **Capability Production Document**. Compliance with identified GIG KIPs are analyzed during the development of the **Information Support Plan** (ISP) and **Test and Evaluation Master Plan**, and assessed during **Defense Information Systems Agency Joint Interoperability Test Command** (JITC) joint interoperability certification testing. An interface is designated as a key interface when one or more the following criteria are met:

- The interface spans organizational boundaries.
- The interface is mission critical.
- The interface is difficult or complex to manage.
- There are capability, interoperability, or efficiency issues associated with the interface.
- The interface impacts multiple acquisition programs.

Program manager compliance with applicable GIG KIPs is demonstrated through inspection of **Joint Capabilities Integration and Development System** (JCIDS) documentation and test plans, and during JITC interoperability certification testing (see [CJCS Instruction 3170.01](#) and [CJCS Instruction 6212.01](#) for detailed discussions of the process).

KIPs are being defined to specify the interfaces to the **Core Enterprise Services** (CES). Compliance with these KIPs is a mandatory element of the **Net-Ready Key Performance Parameter** (NR-KPP). The KIP specifications are in various states of maturity and may be viewed at <http://kips.disa.mil> (user registration required).

Guidance

- **G1630**: Comply with the applicable **Global Information Grid** (GIG) **Key Interface Profiles** (KIPs) for implemented **Core Enterprise Services** (CES) in the Node.
- **G1631**: Expose **Core Enterprise Services** (CES) that comply with the applicable **Global Information Grid** (GIG) **Key Interface Profiles** (KIPs) in all Node services **proxies**.

Best Practices

- **BP1685**: For **Key Interface Profile** (KIP) specifications that are not available or insufficiently mature, implement a "best effort" by following the published intent of functionality and monitor or participate in the relevant specification development body.

Examples

GIG Key Interface Profiles (KIPs) provide a net-centric oriented approach for managing interoperability across the GIG based on the configuration control of key interfaces.

<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Refined Operational View <input checked="" type="checkbox"/> Refined System View <input checked="" type="checkbox"/> Interface Control Specifications -- Interface Control Document (ICD) <input checked="" type="checkbox"/> Technical View & SV-TV Bridge <input checked="" type="checkbox"/> Configuration Management Plan <input checked="" type="checkbox"/> Procedures for standards conformance and interoperability testing utilizing reference implementations <input checked="" type="checkbox"/> Engineering Management Plan 	<table border="1"> <tr> <td colspan="2"><u>Communications RIFs</u></td> </tr> <tr> <td>1.</td> <td>Logical Networks to DSN Transport Backbone</td> </tr> <tr> <td>2.</td> <td>Space to Terrestrial Interface</td> </tr> <tr> <td>3.</td> <td>TTF to Coalition</td> </tr> <tr> <td>4.</td> <td>TTF Component to TTF Headquarters</td> </tr> <tr> <td>5.</td> <td>Teleport (i.e., deployed interface to DSN)</td> </tr> <tr> <td>6.</td> <td>Joint Interconnection Service</td> </tr> <tr> <td>7.</td> <td>DSN Service Delivery Node</td> </tr> <tr> <td>8.</td> <td>Secure Backbone Service Delivery Node (e.g., SCDC/Global RIF)</td> </tr> <tr> <td colspan="2"><u>Computing RIFs</u></td> </tr> <tr> <td>9.</td> <td>Application Server to Database Server</td> </tr> <tr> <td>10.</td> <td>Client to Server</td> </tr> <tr> <td>11.</td> <td>Applications to COE/CP (NCS/SES)</td> </tr> <tr> <td colspan="2"><u>Network Operations RIFs</u></td> </tr> <tr> <td>12.</td> <td>End System to IPD</td> </tr> <tr> <td>13.</td> <td>Management Systems to (Integrated) Management Systems</td> </tr> <tr> <td>14.</td> <td>Management Systems to Managed Systems</td> </tr> <tr> <td>15.</td> <td>EDM to Distribution Infrastructure</td> </tr> <tr> <td>16.</td> <td>Information Services to EDM Infrastructure</td> </tr> <tr> <td colspan="2"><u>Applications</u></td> </tr> <tr> <td>17.</td> <td>Application Server to Shared Data - RIOP (SADI)</td> </tr> </table>	<u>Communications RIFs</u>		1.	Logical Networks to DSN Transport Backbone	2.	Space to Terrestrial Interface	3.	TTF to Coalition	4.	TTF Component to TTF Headquarters	5.	Teleport (i.e., deployed interface to DSN)	6.	Joint Interconnection Service	7.	DSN Service Delivery Node	8.	Secure Backbone Service Delivery Node (e.g., SCDC/Global RIF)	<u>Computing RIFs</u>		9.	Application Server to Database Server	10.	Client to Server	11.	Applications to COE/CP (NCS/SES)	<u>Network Operations RIFs</u>		12.	End System to IPD	13.	Management Systems to (Integrated) Management Systems	14.	Management Systems to Managed Systems	15.	EDM to Distribution Infrastructure	16.	Information Services to EDM Infrastructure	<u>Applications</u>		17.	Application Server to Shared Data - RIOP (SADI)
<u>Communications RIFs</u>																																											
1.	Logical Networks to DSN Transport Backbone																																										
2.	Space to Terrestrial Interface																																										
3.	TTF to Coalition																																										
4.	TTF Component to TTF Headquarters																																										
5.	Teleport (i.e., deployed interface to DSN)																																										
6.	Joint Interconnection Service																																										
7.	DSN Service Delivery Node																																										
8.	Secure Backbone Service Delivery Node (e.g., SCDC/Global RIF)																																										
<u>Computing RIFs</u>																																											
9.	Application Server to Database Server																																										
10.	Client to Server																																										
11.	Applications to COE/CP (NCS/SES)																																										
<u>Network Operations RIFs</u>																																											
12.	End System to IPD																																										
13.	Management Systems to (Integrated) Management Systems																																										
14.	Management Systems to Managed Systems																																										
15.	EDM to Distribution Infrastructure																																										
16.	Information Services to EDM Infrastructure																																										
<u>Applications</u>																																											
17.	Application Server to Shared Data - RIOP (SADI)																																										

11188

P1174: Integrated Architectures

The **DoD Architecture Framework** (DoDAF), available via the DoDAF 1.5 Final Release Quick Link on the [DoD Architecture Registry System Welcome Page](#), provides the rules, guidance, and product descriptions for developing and presenting architecture descriptions to ensure a common denominator for understanding, comparing, and integrating architectures. An integrated architecture consists of multiple views or perspectives (**Operational View** [OV], **Systems and Services View** [SV], **Technical Standards View** [TV] and **All-Views** [AV]) that facilitate integration and promote interoperability across capabilities and among related integrated architectures.

- The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions.
- The SV is a description, including graphics, of systems and interconnections providing for, or supporting, DoD functions.
- The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.
- The AV products provide information pertinent to the entire architecture but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture.

The **GIG** architecture describes the basic, high level architecture in which Nodes reside. It is an integrated architecture consisting of the various DoDAF views. It provides a common lexicon and defines a basic infrastructure for the performance of information exchanges with other Global Information Grid (GIG) Nodes using the **GIG Enterprise Services** (GES) and the **Net-Centric Enterprise Services** (NCES). The GIG Architecture can be viewed <https://disain.disa.mil/ncow/gigv2/index.htm>; the home page for both the GIG architecture and **Net-Centric Operations and Warfare Reference Model** (NCOW RM) is <https://disain.disa.mil/ncow.html> (user registration required for both sites).

Guidance

- **G1635**: Make Nodes that will be part of the **Global Information Grid** (GIG) consistent with the *GIG Integrated Architecture*.

P1175: Core Enterprise Services (CES)

Core Enterprise Services include the following:

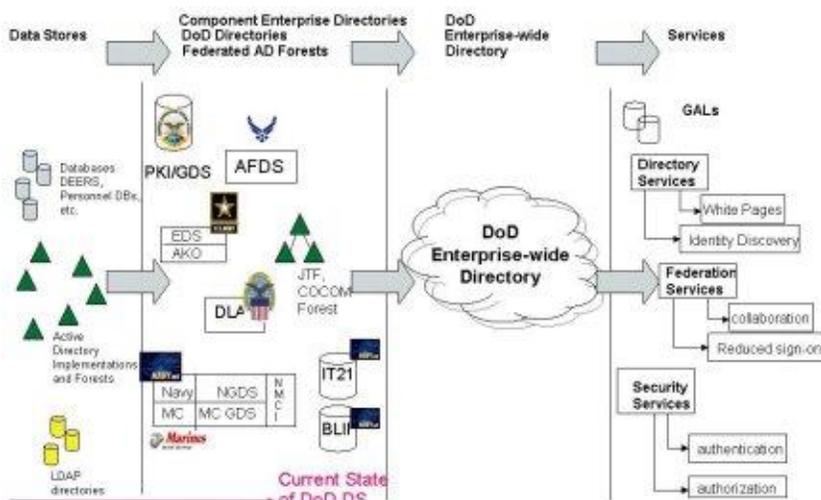
- [Directory Services](#)
- [Security Services](#)
- [Services Management](#)
- [Service Discovery](#)
- [Content Discovery Services](#)
- [Mediation Services](#)
- [Collaboration Services](#)
- [Machine-to-Machine Messaging](#)

P1176: Directory Services

Secure inter-node interoperability relies heavily on the ability to lookup information about people and objects or devices across the breadth of the **Global Information Grid (GIG)**. The technology that supports this is called **directory services**. In the **Net-Centric Enterprise Services (NCES)** service taxonomy, this falls under the scope of the CES **Discovery Service** for person and device discovery.

Nodes routinely use directory services today, such as Microsoft **Active Directory** and the DoD **Public Key Infrastructure (PKI) Global Directory Service (GDS)**. Although implementations are widespread across the GIG, there is limited coordination and synchronization, creating pockets of information that must be unified. There are also substantial differences among implementations, including naming conventions. This situation is made more complex by the fact that these directories are typically also integral to a Node's security and system administration, supporting such basic functions as user login.

Coordination efforts at the level of the GIG within the DoD are underway to address these challenges. The DoD CIO directed DISA to develop a roadmap for directory services for the GIG. That roadmap is in draft form and is the product of the Joint Enterprise Directory Services Working Group (JEDIWG), which maintains a Web site at <https://gesportal.dod.mil/sites/JEDIWG/default.aspx> (user registration required). This working group oversees both the **Joint Directory Services Working Group (JDSWG)** that focuses on PKI related requirements addressed by the **Global Directory Service (GDS)** as well as the **DoD Active Directory Interoperability Working Group (DADIWG)**. A snapshot of directory services evolution is in the diagram below:



I1189

Guidance

- **G1625:** Provide a **commercial off-the-shelf** Directory Service that all of the **Components** of a Node can use.
- **G1637:** Make Node-implemented **directory services** comply with the directory services **Global Information Grid (GIG) Key Interface Profiles (KIPs)**.
- **G1638:** Comply with the directory services **Global Information Grid (GIG) Key Interface Profiles (KIPs)** in Node directory services **proxies**.

Best Practices

Part 4: Node Guidance

- **BP1686**: Align Node interfaces to **Components** for directory services with the guidance being provided by the Joint Enterprise Directory Services Working Group (JEDIWG) and sub-working groups, including such guidance as naming conventions, federation, and synchronization.
- **BP1687**: Follow **Active Directory** naming conventions defined in the *Active Directory User Object Attributes Specification* as required by the DoD **CIO** memorandum titled *Microsoft Active Directory (AD) Services*.

P1177: Security Services

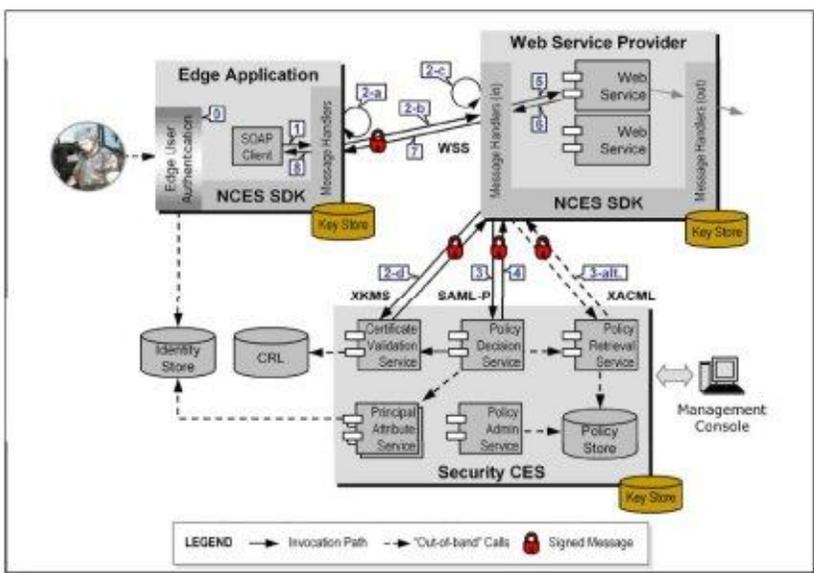
Net-centric information exchanges require security. The security mechanisms must be understood and implemented **Global Information Grid (GIG)**-wide because the information exchanges may occur between any Nodes on the GIG.

The **CES** approach to providing these GIG-wide security mechanisms is based on the DoD **Public Key Infrastructure (PKI)**. Several security services in multiple categories of functionality are defined or planned, as shown in the following table. Generally, these services add to the DoD PKI authentication capabilities, providing a more complete set of security capabilities to applications, infrastructure, or other services.

Security Service Categories	Current Services	Future Services
Credential Management Services	Certificate Validation Service	Certificate Retrieval Service Certificate Registration Service
Authorization Services	Policy Decision Service Policy Retrieval Service Policy Administration Service	Policy Subscription Service
Attribute Services	Principal Attribute Service	Resource Attribute Service Environment Attribute Service
Security Context Services	None	Security Context Service
Auditing and Logging Services	None	Security Logging Service Auditing Service

The figure below shows the relationship and typical interactions of these elements for a nominal Web client invocation of a Web service. Node implementation of the elements shown below presents some critical design choices. The figure does not show, for instance, where each of the elements found in the **Security CES** box are hosted. There is active debate over this and related topics.

Authorization decisions should be the local purview of the Nodes, based on **enterprise** standards for identity, attributes, and policies, augmented and tailored locally to suit any unique requirements a Node may have. Furthermore, because security decisions can be computationally intensive and frequent, locally hosted implementations may be warranted by performance. Therefore, CES Security Services for authorization and policy decisions should be hosted locally on a Node. This requires coordination with DISA to implement these services on the local Node, and the overall approach may change as the Security Services are more fully developed and piloted.



11190

Detailed Perspectives

Implementation topics for near term consideration are identity management, authentication, and authorization.

- [Identity Management](#)
- [Public Key Infrastructure](#) (authentication and authorization)

P1178: Identity Management

Identity is an essential part of the **CES** Security Services, but **Identity Management** is not addressed in CES Increment 1. Identities of **Global Information Grid** (GIG) entities, human and non-human (i.e., services), must be unique across the GIG. DoD **PKI X.509 certificates** reserve a field to contain identity data, but there are issues today with how that field is populated for certain populations of users (e.g., coalition partners), and how to handle non-person entities.

While a universal solution for Identity Management is not yet defined, it is possible to make progress in the implementation of these services, particularly for Web applications and services with U.S. users having a Common Access Card (**CAC**) holding DoD PKI X.509 certificates.

Identity is not as well understood and defined for non-person entities, such as services that may be part of a long invocation chain that is part of a workflow or orchestrated to yield a specific answer to a service invocation. Web server credentialing, though, has been defined to rely upon the DNS name of the site for identification.

The **Net-Centric Enterprise Services** (NCEs) and **Public Key Infrastructure** (PKI) Program Offices are working on the challenges of non-person Identity Management, and an request for information has been issued to identify potential solutions.

Guidance

- [G1652](#): Use DoD **PKI X.509 certificates** for **servers**.

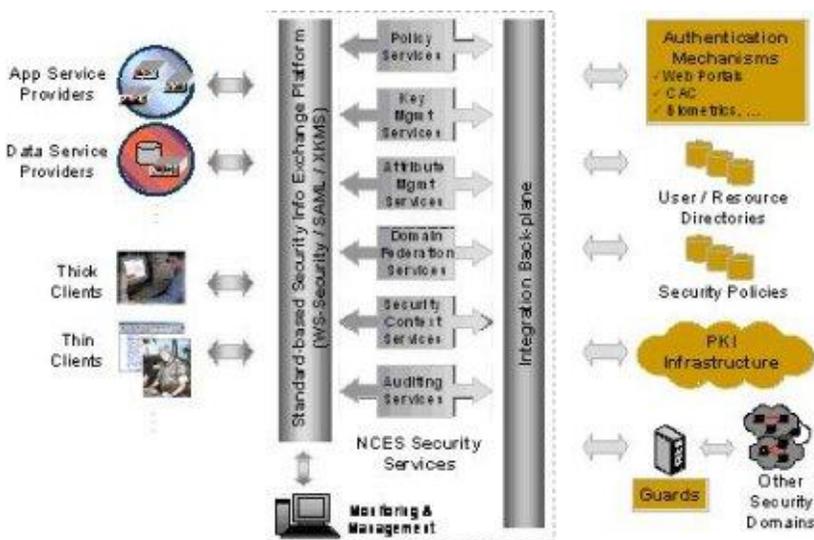
P1179: Public Key Infrastructure

Net-Centric Enterprise Services (NCES) Security Services rely heavily on **Public Key Infrastructure (PKI)** and **Public Key (PK) Enabling (PK-Enabling)**. PKI provides an assured way for enabled applications to authenticate both intra-node and inter-node. PKI supports the concept of a single login across the **enterprise**, but legacy non-PK-enabled applications and services mean that username and password synchronization is also needed to support the single login concept; however, this is only practical in a limited sense (i.e., not the entire **GIG**). There remain some PKI implementation challenges, such as the implementation of the process for validating that an entity's **certificate** has not been revoked. Some COTS products, including some Web Application Containers, do not support the use of the **Online Certificate Status Protocol (OCSP)** or do not provide a capability to do file-based checking of the older **Certificate Revocation List (CRL)**.

Nodes having both DoD and **Intelligence Community (IC)** systems and networks will also face the fact that the DoD and IC have implemented separate PKIs (including the dependent Directory Services). In general, the DoD PKI operates on the collateral classification networks, and the IC PKI operates on the **SCI** classified networks. Nodes may have to interface with multiple PKIs, therefore, depending on the systems and security levels at the Node. This presents some additional challenges when cross-domain interoperation is required, whether intra- or inter-node.

Nodes that have multinational or coalition personnel accessing the system will also encounter a challenge in obtaining CACs containing PKI certificates for these persons. The process is not well defined. As DoD moves further into the net-centric concepts, obtaining certificates for non-human entities in multinational or coalition systems will also be a challenge.

Authorization based on **attributes** corresponding to an entity is a practical way to implement authorization, provided that the enterprise can agree on the definitions of the attributes, policy, and a way of securely communicating and validating role membership. Unfortunately, attribute definitions and common security policy are not defined yet for the **Global Information Grid (GIG)**, and Nodes are forced to use interim approaches, such as Windows **AD** or **NIS** group memberships, and evolve to a uniform definition of GIG roles and policies. Federation has not been addressed sufficiently to provide specific guidance.



11191

P1180: Services Management

Net-centric operations can create mutual, mission-dependent obligations between Nodes. **Service Management** affects Node interoperability in that failure to provide services according to advertised capabilities or negotiated **Service Level Agreements** (SLAs) is essentially non-interoperability in the performance dimension.

Net-Centric Enterprise Services (NCES) services management capabilities are under development, but, as indicated in the current NCES schedule, are not scheduled for fielding until **CES** Increment 2.

Best Practices

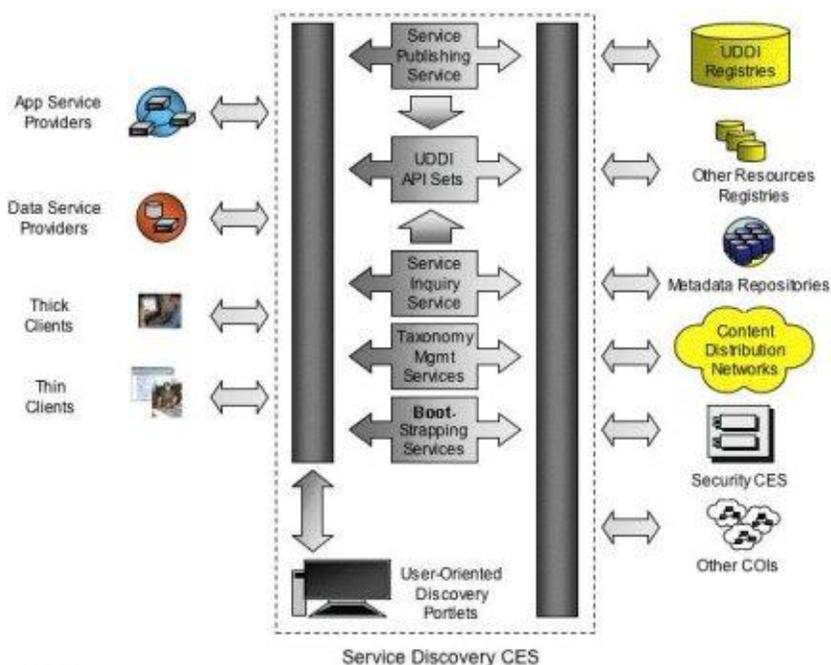
- [BP1688](#): For **Services Management**, use an interim solution of instrumentation of services and external monitoring.

P1181: Service Discovery

Loosely coupled, net-centric information and services must be discoverable. That is, Nodes and **Components** must be able to discover dynamically where Component services and information reside in the **Global Information Grid (GIG)** and bind to those providers at runtime. The **discovery** concept relies upon the use of registries that are human and machine usable, for maintaining **metadata** descriptions of information and services.

Net-Centric Enterprise Services (NCES) includes **Service Discovery (SD)** services. Scheduled for CES Increment 1 fielding, a pilot implementation of SD services is available. The construction of registry entries is specified by the **Service Definition Framework (SDF)**. The following figure shows the overall SD services architecture. Web **portlets** are being developed to assist in using the service, providing support for service publishing, searching, and browsing. The service registry implementation uses the **Universal Description, Discovery, and Integration (UDDI)** registry underneath, and the portlets use the UDDI **application programming interface (API)**. A *Service Discovery Portlet Users Guide* describes how to use the portlets to access the registry.

Nodes face several implementation choices regarding the alignment of Component and Node approaches to SD. Components exposed by the Node should be described as specified by the SDF and registered with the DISA hosted registries so that the Components services are visible to other Nodes. Use the pilot program to practice and exercise the mechanics of service discovery and late binding. If the pilot implementation is not reachable, such as might be the case in a higher classified environment, the Node managers should coordinate among themselves and DISA to provide pilot and full service implementations that are reachable. Internal-facing services that are not likely to be of value beyond the Node's boundaries do not have to be discoverable, though it is a recommended best practice. If used internally, implement service discovery for high availability.



I1192

Guidance

- **G1639:** Describe **Components** exposed by the Node as specified by the **Service Definition Framework**
- **G1640:** Register **Components** exposed by the Node with the **DISA**-hosted registries.
- **G1641:** Comply with the Service Discovery **Global Information Grid (GIG) Key Interface Profiles (KIPs)** in Node-implemented **Service Discovery (SD)**.

Part 4: Node Guidance

- [G1642](#): Comply with the **Service Discovery Global Information Grid (GIG) Key Interface Profiles (KIPs)** in Node Service Discovery (SD) **proxies**.

Best Practices

- [BP1689](#): Use the **Service Discovery (SD)** pilot program to practice and exercise the mechanics of service discovery and late binding.
- [BP1690](#): Use Node implemented **Service Discovery (SD)** for high availability.
- [BP1691](#): Use **Node** implemented **Service Discovery (SD)** to meet compartmentalization needs.

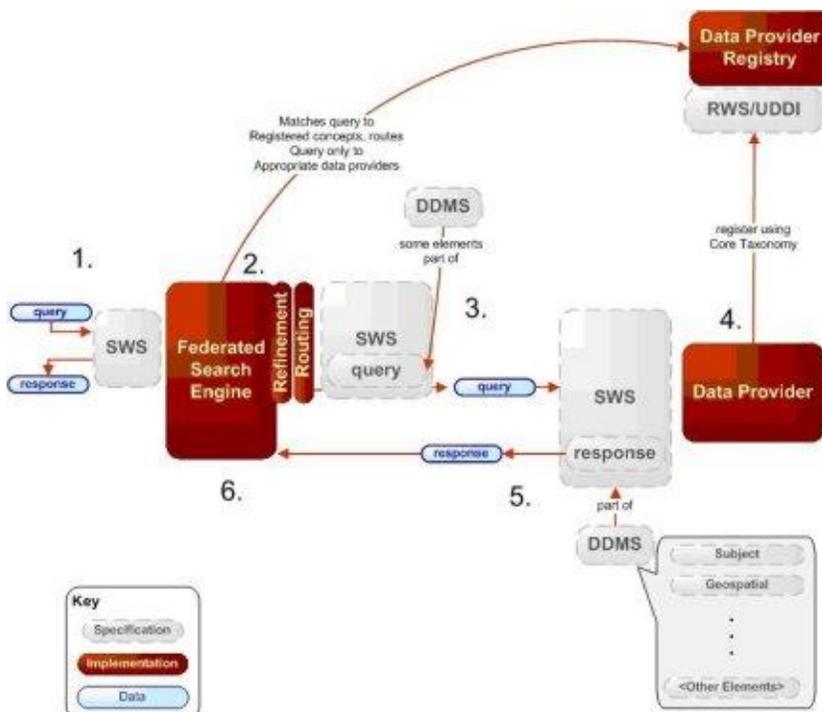
P1182: Content Discovery Services

Net-Centric Enterprise Services (NCES) includes a **Content Discovery Service** (CDS) that provides a **Federated Search** capability. That is, the service can search across a set of Content Discovery Services and yield an integrated result. The current approach to providing this service is to harness an existing capability termed "Federated Search" developed under the **Horizontal Fusion** (HF) program. The capability utilizes the **DoD Discovery Metadata Specification** (DDMS).

The Federated Search and DDMS document contains the following information:

Federated Search is implemented as a set of cooperating Web services. These services talk to each other using a common specification. The specification defines how a query and the results from that query are communicated. It describes not only the meaning, but also the format of the data that is exchanged between the services. The Defense Discovery Metadata Specification (DDMS) is used in the Federated Search specification to represent the concepts of a query as well as the resource result records, called meta cards, generated by a search result. Outgoing queries are matched against the resource meta cards by data providers to generate search results. It is the DDMS that ties the queries to the results and is used to express a common vocabulary.

The following figure shows the Horizontal Fusion program's implementation of this Federated Search capability. Each Node should implement **Federated Search - Registration Web Service** (RWS) and **Search Web Service** (SWS). The RWS is used by data producers to register content sources and the SWS is used to search for content from the registered sources.



11193

Guidance

- **G1643:** Comply with the **Federated Search # Registration Web Service** (RWS) **Global Information Grid** (GIG) **Key Interface Profiles** (KIPs) in Node implemented Federated Search # Registration Web Service (RWS).
- **G1644:** Comply with the **Federated Search # Search Web Service** (SWS) **Global Information Grid** (GIG) **Key Interface Profiles** (KIPs) in Node implemented Federated Search # Search Web Service (SWS).
- **G1645:** Implement a local **Content Discovery Service** (CDS).

Part 4: Node Guidance

- [G1646](#): Comply with the directory services **Global Information Grid (GIG) Key Interface Profiles (KIPs)** in Node **Federated Search** Services **proxies**.
- [G1647](#): Provide access to the **Federated Search** Services.

Best Practices

- [BP1648](#): Host the **Registration Web Service** (RWS) registration **portlet** in the Node.
- [BP1865](#): Provide sufficient program, project, or initiative **metadata** descriptions and automated support to enable **mediation** and translation of the data between **interfaces**.

P1183: Mediation Services

Published information may not always be in a format compatible with the subscriber's needs. The CES Mediation Service currently provides a capability to translate **XML** documents from one **schema** into another. To do this, the service uses **XSL Transformations** (XSLT) and mappings DoD Metadata Registry. When XML document translation between schemas is a necessity, use the **CES** Mediation Service or a locally hosted copy thereof. Register developed mappings in the **DoD Metadata Registry**.

Best Practices

- **BP1711**: Use the **CES** Mediation Service, or a locally hosted copy, when **XML** document translation between **schemas** is a necessity.
- **BP1712**: Register developed mappings in the **DoD Metadata Registry**.

P1184: Collaboration Services

Collaboration tools provide a virtual meeting room environment for human interaction. The virtual environment enables multimedia collaboration (text, voice, and video) in multiple modes (person-to-person, open chat, restricted meeting, etc.) and application broadcasting and sharing.

The **DISA Joint Interoperability Test Command** (JITC) has validated suite of collaboration tools and standards called the **Defense Collaboration Tool Suite** (DCTS) for interoperability and operational use. The DCTS **Collaboration Management Office** (CMO) within DISA is responsible for fielding, sustaining, and managing the life cycle of DCTS. Collaboration products approved for interoperability are listed at <http://jitc.fhu.disa.mil/washops/jtcd/dcts/status.html>. Products certified for use on **Secret Internet Protocol Router Network** (SIPRNet) are listed at <http://jitc.fhu.disa.mil/washops/jtcd/dcts/projects.html>.

The recent DOD CIO memorandum, "DoD Collaboration Policy Update," requires use of the **NCES** Collaboration Services that are under development. It also provides policy for urgent requirements until the NCES services are operational. Collaboration products used to satisfy urgent requirements should be approved and from the list on the aforementioned Web sites, until the NCES Collaboration Service is available.

Best Practices

- **BP1692:** Determine which Collaboration Service vendor offering to employ in a disadvantaged environment or separate network.
- **BP1693:** Make sure that **collaboration** products used to satisfy urgent requirements are from the **JTIC** list.

P1185: Machine-to-Machine Messaging

Net-Centric Enterprise Services (NCES) is defining services for **machine-to-machine messaging**, similar in capability to services offered by several COTS vendors of **Enterprise Service Busses** (ESBs). ESBs, though, are not yet interoperable enough to support messaging between arbitrary **Global Information Grid** (GIG) Nodes using different ESBs.

Guidance and Best Practice Details

G1085

Statement:

Establish a **registered namespace** in the **XML Gallery** in the **DoD Metadata Registry** for all DoD Programs.

Rationale:

A **registered namespace** permits unique identification and categorization of a Program which avoids name collisions and conflicts. The DoD Net-Centric Data Strategy requires storing data products in shared spaces to provide access to all authorized users and tagging these data products with **metadata** to enable discovery of data by authorized users. The use of a unique **registered namespace** provides an absolute identifier to products associated with a particular product and is an **XSD** schema requirement.

Referenced By:

Design Tenet: Open Architecture
Design Tenet: Service-Oriented Architecture (SOA)
Maintainability
WSDL
Using XML Namespaces
Interoperability

Evaluation Criteria:

1) Test: [G1085.1]

Does the Program have an assigned namespace in the **DoD Metadata Registry**?

Procedure:

Check the **DoD Metadata Registry** to determine whether program is associated with **COI(s)**.

Example:

None

G1125

Statement:

Use the **Department of Defense Metadata Specification (DDMS)** for standardized tags and taxonomies.

Rationale:

These standardized tags or Metacards will be developed, maintained, and placed under configuration as appropriate and will comply with the **DDMS** and **COI** guidance. These include specifications defining the tagging for security classification and dissemination control. See the DoD Discovery Metadata Specification Web site (<http://metadata.dod.mil/mdr/irs/DDMS/>) for the current **DDMS** standards.

Referenced By:

Design Tenet: Service-Oriented Architecture (SOA)
Design Tenet: Make Data Visible
Design Tenet: Provide Data Management
Design Tenet: Open Architecture
Metadata Registry
Design Tenet: Accommodate Heterogeneity
Interoperability

Evaluation Criteria:

1) Test: [G1125.1]

Has the Program documented the profile used for published data assets in accordance with guidance?

Procedure:

Check the DoD Metadata Registry to determine whether the program is associated with **COI(s)**.

Example:

None

G1382

Statement:

Be associated with one or more **Communities of Interest (COIs)**.

Rationale:

The DoD Net-Centric Data Strategy emphasizes the establishment of Communities of Interest (**COIs**). This strategy introduces management of data within Communities of Interest (COIs) rather than standardizing **data elements** across the DoD. Thus all DoD Programs must map to one or more COIs. DoD Programs should participate in COIs as a normal course of doing business. They will identify relevant COIs; actively collaborate with them to promote reuse and cross-coordination of **metadata**; sponsor participation of system developers in the COI process and where appropriate contribute engineering expertise to the COI as a stakeholder. New programs should include community collaboration requirements in acquisition documents as required.

Referenced By:

Design Tenet: Make Data Interoperable
Design Tenet: Be Responsive to User Needs
Design Tenet: Make Data Understandable
Reusability
Metadata Registry
Interoperability

Evaluation Criteria:

1) **Test:** [G1382.1]

Is the Program associated with a **COI**?

Procedure:

Check the DoD Metadata registry to determine whether program is associated with any **COI(s)**.

Example:

None

G1383

Statement:

Use a **registered namespace** in the XML Gallery in the **DoD Metadata Registry**.

Rationale:

The use of the **DoD Metadata Registry** helps to avoid name collisions and conflicts.

The assignment of a unique **registered namespace** permits a program to be uniquely identified and categorized. The DoD's Net-Centric Data Strategy requires that data products be stored in shared spaces to provide access to all authorized users and that these data products be tagged with **metadata** to enable discovery of data by authorized users. The use of a unique registered namespace provides an absolute identifier to products associated with a particular product and is an **XSD** schema requirement.

Referenced By:

[Interoperability](#)
[Design Tenet: Make Data Understandable](#)
[Design Tenet: Make Data Interoperable](#)
[Reusability](#)
[Metadata Registry](#)
[Design Tenet: Make Data Visible](#)
[Using XML Namespaces](#)
[Design Tenet: Make Data Accessible](#)
[Design Tenet: Make Data Trustable](#)
[Design Tenet: Provide Data Management](#)
[Design Tenet: Be Responsive to User Needs](#)

Evaluation Criteria:

1) Test: [G1383.1]

Does the Program have an assigned namespace for its XML data assets?

Procedure:

Check **DoD Metadata Registry** to determine whether the Program is associated with **COI(s)**.

Example:

None

G1384

Statement:

Review **XML Information Resources** in the **DoD Metadata Registry**, using those which can be reused.

Rationale:

The DoD Net-Centric Data Strategy requires that **XML** information resources within a **COI** in the **DoD Metadata Registry** be examined by DoD projects for possible reuse to help foster common standards within a **COI** and promote interoperability.

Note: *The proposed DoD Metadata Registry tools have not been formally released. The Beta version thereof is in testing. Automatic Waivers of this requirement will be permitted until the tools are formally released.*

Referenced By:

Design Tenet: Make Data Interoperable
Interoperability
Reusability
Design Tenet: Provide Data Management
Design Tenet: Make Data Understandable
Design Tenet: Be Responsive to User Needs
Metadata Registry
Using XML Namespaces

Evaluation Criteria:

1) Test: [G1384.1]

Has the program reused information resources from the **DoD Metadata Registry**?

Procedure:

Check the **XSDs** associated with the program to determine whether XSDs referenced by other namespaces have been used. Check the **DoD Metadata Registry** to determine whether the Program has registered the reuse of XML information resources belonging to other namespaces. Reuse is indicated by formally subscribing to selected components in the registry.

Example:

None

G1385

Statement:

Identify **XML Information Resources** for registration in the XML Gallery of the **DoD Metadata Registry**.

Rationale:

The DoD Net-Centric Data Strategy requires that **XML Information Resources** developed during the course of a program be identified, examined for usefulness by other DoD Programs in the same or related **COIs** and be submitted for inclusion in the XML Gallery of the **DoD Metadata Registry**.

Referenced By:

Design Tenet: Provide Data Management
Design Tenet: Make Data Interoperable
Metadata Registry
Design Tenet: Make Data Trustable
Interoperability
Design Tenet: Make Data Visible
Design Tenet: Make Data Accessible
Using XML Namespaces
Reusability

Evaluation Criteria:

1) Test: [G1385.1]

Has the Program submitted new information resources to the **DoD Metadata Registry**?

Procedure:

Check the **XSDs** associated with the program namespace to determine whether they have been registered in the **DoD Metadata Registry** XML Gallery.

Example:

None

G1386

Statement:

Review predefined commonly used **data elements** in the **Data Element Gallery** of the **DoD Metadata Registry**, using those in the **relational database** technology which can be reused in the Program.

Rationale:

The DoD Net-Centric Data Strategy requires that DoD Programs examine data element information resources within a **COI** in the **DoD Metadata Registry** for possible reuse to help foster common standards within a **COI** and promote interoperability. Elements include **US State Codes** and **Country Codes**. This reuse is preferential to reusing existing industry standard **data elements** or developing new **data elements**.

Referenced By:

Design Tenet: Provide Data Management
Design Tenet: Be Responsive to User Needs
Reusability
Design Tenet: Make Data Understandable
Interoperability
Metadata Registry
Design Tenet: Make Data Interoperable

Evaluation Criteria:

1) Test: [G1386.1]

Has the Program reused common database elements?

Procedure:

Check the DoD Metadata Registry Data Element Gallery to determine whether the program has registered database elements for reuse. Reuse is indicated by formally subscribing to selected components in the registry.

Check the program database to see whether registered have been included therein.

Example:

None

G1387

Statement:

Identify **data elements** created during Program development for registering in the **Data Element Gallery** of the **DoD MetaData Registry**.

Rationale:

The DoD Net-Centric Data Strategy requires that Programs identify and examine developed **data elements** for usefulness by other DoD Programs in the same or related **COIs** and submit the data elements for inclusion in the **Data Element Gallery** of the **DoD Metadata Registry**.

Referenced By:

Design Tenet: Make Data Visible
Interoperability
Metadata Registry
Design Tenet: Make Data Accessible
Design Tenet: Make Data Trustable
Design Tenet: Provide Data Management
Reusability

Evaluation Criteria:

1) Test: [G1387.1]

Has the Program submitted common database elements to the **DoD Metadata Registry**?

Procedure:

Check the [DoD Metadata Registry](#) Data Element Gallery to determine whether the program has submitted database elements for reuse.

Example:

None

G1388

Statement:

Use predefined commonly used database tables in the **DoD Metadata Registry**.

Rationale:

The DoD Net-Centric Data Strategy requires that DoD Programs examine data table information resources within a **COI** in the **DoD Metadata Registry** for possible reuse to help foster common standards within a COI and promote interoperability. This reuse is preferable to reusing existing industry standard **data elements** or developing new data elements. Some examples are **Country Code**, **US State Code**, **Purchase Order Type Code**, **Security Classification Code**. These tables are found in the **Reference Data Set** Gallery of the DoD Metadata Registry.

Referenced By:

Design Tenet: Make Data Understandable
Design Tenet: Be Responsive to User Needs
Metadata Registry
Reusability
Interoperability
Design Tenet: Make Data Trustable
Design Tenet: Make Data Interoperable

Evaluation Criteria:

1) **Test:** [G1388.1]

Has the Program reused common database tables?

Procedure:

Check the DoD Metadata Registry to determine whether the program has registered database tables for reuse. Reuse is indicated by formally subscribing to selected components in the registry.

Check the program database to see whether registered data tables have been included therein.

Example:

None

G1390

Statement:

Standardize on the terminology published by relevant **Communities of Interest (COIs)** listed in the **Taxonomy Gallery** of the **DoD Metadata Registry**.

Rationale:

A **taxonomy** partitions the body of knowledge associated with a **Community of Interest COI** and defines the relationships among component parts. A taxonomy permits classification of concepts associated with a COI. This in turn provides categories and definitions for discovery tags which aids in information use and retrieval by authorized users. Program use of COI taxonomies occurs in several places:

1. Taxonomy used to describe information services for discovery.
2. Taxonomies created by the COI as a means to extend the **DoD Discovery Metadata Specification (DDMS)** for data asset discovery.
3. Taxonomies used to support mediation.

Referenced By:

Design Tenet: Make Data Understandable
Design Tenet: Make Data Interoperable
Design Tenet: Provide Data Management
Metadata Registry
Design Tenet: Make Data Accessible
Design Tenet: Be Responsive to User Needs

Evaluation Criteria:

1) Test: [G1390.1]

Has the Program adhered to the standard **taxonomies** for the **COIs** associated with the program?

Procedure:

Check the DoD Metadata Registry and Taxonomy Gallery to determine whether taxonomies exist for the COI in which the Program resides.

Example:

None

G1391

Statement:

Identify **taxonomy** additions or changes in conjunction with the **Communities of Interest (COIs)** during the Program development for potential inclusion in the **Taxonomy Gallery** of the **DoD Metadata Registry**.

Rationale:

DoD Programs associated with a specific COI need to identify and submit potential taxonomy changes or additions to the **DoD Metadata Registry** to maintain an accurate and effective taxonomy within the **COI**.

Referenced By:

Design Tenet: Make Data Visible
Design Tenet: Make Data Accessible
Design Tenet: Be Responsive to User Needs
Design Tenet: Make Data Interoperable
Metadata Registry
Design Tenet: Make Data Understandable

Evaluation Criteria:

1) Test: [G1391.1]

Has the Program submitted **taxonomy** additions or changes to the **DoD Metadata Registry**?

Procedure:

Check the DoD Metadata Registry and to determine whether the program has submitted taxonomy changes for reuse.

Example:

None

G1569

Statement:

Maintain a comprehensive list of all of the **Components** that are part of the Node.

Rationale:

Throughout the lifecycle of a Node (from design to instantiation), this action is fundamental to the provisioning of a shared infrastructure and the avoidance of functional duplication within the Node. This activity has a direct impact on the design and implementation requirements during acquisition.

Referenced By:

[Interoperability](#)
[Design Tenet: Service-Oriented Architecture \(SOA\)](#)
[Reusability](#)
[Nodes as Stakeholders](#)
[Design Tenet: Enterprise Service Management](#)

Evaluation Criteria:

1) **Test:** [G1569.1]

Is there a list of Components that comprise the Node?

Procedure:

Examine the documents (for example, the Node's design requirements) and look for a list of Components.

Example:

None.

G1570

Statement:

Assume an active management role among the **Components** within the Node.

Rationale:

Involvement of the Node as a stakeholder in its Components (from design to instantiation) has a bearing on **Global Information Grid** (GIG) interoperability. Strong coordination among a Node's Components will likely avoid the external exposure of inconsistencies or, worse, incomplete, inaccurate, or misunderstood data.

Referenced By:

[Nodes as Stakeholders Interoperability](#)

Evaluation Criteria:

1) Test: [G1570.2]

Do the Components of the Node set forth requirements in their [appropriate acquisition document] for coordinating with the Node.

Procedure:

Check the [appropriate acquisition document] of the Components and determine if the Node is listed as a stakeholder or if there are requirements for coordinating with the Node.

Example:

A Component's **Capability Development Document (CDD)** may state a requirement for participating in a Node which could satisfy this requirement.

2) Test: [G1570.1]

Do the Components of the Node list the Node as a primary stakeholder in their [appropriate acquisition document]?

Procedure:

Check the [appropriate acquisition document] of the Components and determine if the Node is listed as a stakeholder or if there are requirements for coordinating with the Node.

Example:

A Component's **Capability Development Document (CDD)** may state a requirement for participating in a Node which could satisfy this requirement.

G1571

Statement:

Maintain a comprehensive list of all the **Communities of Interest** (COIs) to which the **Components** of a Node belong.

Rationale:

The Node infrastructure must be engineered to support the information exchange between **Communities of Interests** (COIs). If a comprehensive list of COIs is not created and maintained then the infrastructure may no longer be adequate and may continue to make provisions for COIs that are no longer a part of the Node.

Referenced By:

[Net-Centric Information Engineering](#)
[Design Tenet: Be Responsive to User Needs](#)

Evaluation Criteria:

1) Test: [G1571.1]

Do the Node's Components have representation registered within the DoD Metadata Registry as members of the Communities of Interest (COIs)?

Procedure:

Examine the DoD Metadata Registry for members of the Node organization that are members of the pertinent COIs.

Example:

None.

G1572

Statement:

Include the Node as a party to any **Service Level Agreements** (SLAs) signed by any of the **Components** of the Node.

Rationale:

The Node has a stake in performance specifications provided in the **Service Level Agreements** (SLA). Since the SLA is a contract that commits the application service provider to a required level of service. The Node must be able to support that level of service with its infrastructure.

Referenced By:

[Net-Centric Information Engineering](#)
[Design Tenet: Scalability](#)
[Design Tenet: Availability](#)

Evaluation Criteria:

1) **Test:** [G1572.1]

Does the Node have copies of all Service Level Agreements (SLAs) signed by its Components?

Procedure:

Compare the Service Level Agreements (SLAs) against the service Components supported by the Node.

Example:

None.

G1573

Statement:

Define the enterprise design patterns that a Node supports.

Rationale:

The Node infrastructure must be engineered to support information exchanges between various **Communities of Interest** (COIs). The COIs can require any number of **Components** to fulfill the COIs mission, When a Component wishes to make its data available over the **enterprise**, there are different enterprise design pattern which can be used. For example, the mechanism selected by a Component to exchange information may be publish-subscribe, broker, or client server. The Node infrastructure must support whichever enterprise design pattern mechanism is selected.

Referenced By:

[Design Tenet: Open Architecture](#)
[Design Tenet: Service-Oriented Architecture \(SOA\)](#)
[Net-Centric Information Engineering](#)

Evaluation Criteria:

1) **Test:** [G1573.1]

Does the Node document which types of enterprise design patterns it supports?

Procedure:

Look through the Node documents for a list of enterprise design patterns it supports.

Example:

None.

G1574

Statement:

Define which enterprise design patterns a **Component** requires.

Rationale:

A Component should document which enterprise design patterns it intends to capitalize on to meet its mission. For example, a client interested in using a client-server weather service, could have problems if the weather service is a real-time publish-subscribe service. This action clarifies for the Node which enterprise design patterns are required by its Components and provides direction for which patterns to support at the Node level.

Referenced By:

[Net-Centric Information Engineering](#)
[Design Tenet: Open Architecture](#)
[Design Tenet: Service-Oriented Architecture \(SOA\)](#)

Evaluation Criteria:

1) **Test:** [G1574.1]

Does the Component indicate which type of enterprise design pattern it will use?

Procedure:

Look through the Component documentation and that defines what type of enterprise design pattern it uses.

Example:

None.

G1575

Statement:

Designate Node representatives to relevant **Communities of Interest** (COIs) in which Components of the Node participate.

Rationale:

COI is the inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange. The principal mechanism for recording COI agreements is the **DoD Metadata Registry** required by the DoD CIO Memorandum *DoD Net-Centric Data Management Strategy: Metadata Registration*. There are registry implementations on the Non-secure Internet Protocol Router Network (**NIPRNet**), Secret Internet Protocol Router Network (**SIPRNet**), and Joint Worldwide Intelligence Communications System (**JWICS**).

Referenced By:

[Net-Centric Information Engineering
Design Tenet: Be Responsive to User Needs](#)

Evaluation Criteria:

1) Test: [G1575.1]

Does the Node have representation registered within the Metadata Registry as members of the **Communities of Interest** (COIs)?

Procedure:

Examine the **DoD Metadata Registry** for members of the Node organization that are members of the pertinent COIs.

Example:

None.

G1576

Statement:

Provide an environment to support the development, build, integration, and test of net-centric capabilities.

Rationale:

Nodes should provide an environment to support the development, integration, and testing of net-centric capabilities of its **Components**. As Nodes themselves and the Components within the Nodes move closer to the implementation of net-centric capabilities, it becomes increasingly important to provide a development, integration, and test environment to support those capabilities. This environment should allow for the exercise not just the Node infrastructure, but also either host locally within the Node, or provide access to, **Net-Centric Enterprise Services** (NCES) piloted services. The particulars on how this is done depend on the characteristics of the Node. For example, mobile or deployed Nodes would provide environments substantially different than fixed land-based or permanent Nodes.

Referenced By:

[Internal Component Environment](#)
[CES Definitions and Status](#)
[Maintainability](#)
[Design Tenet: Joint Net-Centric Capabilities](#)

Evaluation Criteria:

1) Test: [G1576.1]

Are there instructions on how to develop, build, integrate or test Components within the Node?

Procedure:

Look for user guides or installation instructions that cover the Node environment.

Example:

None.

G1577

Statement:

Maintain an **Enterprise Service** schedule for interim and final **enterprise** capabilities within the Node.

Rationale:

The current state of **Enterprise Services** is in flux. Developing **Components** that rely on those services can create a circular problem for development. An enterprise service schedule for interim and final capabilities will help elevate the co-dependencies of the Component lifecycle from the Node lifecycle.

Referenced By:

Maintainability
Coordination of Node and Enterprise Services
Internal Component Environment
CES Parallel Development

Evaluation Criteria:

1) Test: [G1577.1]

Is there an enterprise service schedule or roadmap that covers interim and final capabilities of the Node?

Procedure:

Look for the existence of the schedule or a roadmap for the Node.

Example:

None.

G1578

Statement:

Define a schedule for **Components** that includes the use of the **Enterprise Services** defined within the Node's enterprise service schedule.

Rationale:

The exercise of matching those **Enterprise Services** required by the **Component** to those provided by the Node can help identify and gaps in the Node's functionality. By tying the Component's enterprise services to the Node's **enterprise** schedule, critical paths may be identified in the Node's schedule.

Referenced By:

CES Parallel Development
Coordination of Node and Enterprise Services
Maintainability
Internal Component Environment

Evaluation Criteria:

1) Test: [G1578.1]

Does the Component have an enterprise service schedule or roadmap that shows the progression of enterprise service usage by interim and final capabilities of the Component?

Procedure:

Look for the existence of the schedule or a roadmap for the Component.

Example:

None.

G1579

Statement:

Define which **Enterprise Services** the Node will host locally when the Node becomes operational.

Rationale:

Locally defined **Enterprise Services** are inherently faster and less susceptible to network failures and traffic than local services. If a **Component** requires performance based or critical enterprise services that the Node will only provide as a **proxy**, then development, building, integration and testing should be done to the local enterprise service specification. If the Node developed enterprise service will not be ready until near the end of the Component's schedule, take steps to minimize risk.

Referenced By:

[Internal Component Environment](#)
[Design Tenet: Service-Oriented Architecture \(SOA\)](#)

Evaluation Criteria:

1) **Test:** [G1579.1]

Does the Node specification identify which Enterprise Services will be locally defined within the Node?

Procedure:

Review the Node specification for a list of Enterprise Services that will be locally defined within the Node.

Example:

None.

G1580

Statement:

Define which **Enterprise Services** will be hosted over the **Global Information Grid** (GIG) when the Node becomes operational.

Rationale:

Enterprise Services that are defined using **proxies** should have interfaces that follow the standards defined by the enterprise service provider. Therefore, the access to the **server** should be fairly stable and almost static in nature with few changes. These are services that should be in the critical path of a Component's mission.

Referenced By:

Internal Component Environment
Design Tenet: Service-Oriented Architecture (SOA)

Evaluation Criteria:

1) **Test:** [G1580.1]

Does the Node specification identify which Enterprise Services will be defined using proxies?

Procedure:

Review the Node specification for a list of Enterprise Services that will be defined using proxies.

Example:

None.

G1581

Statement:

Expose **legacy system** or **application** functionality through the use of a service that uses a **facade design pattern**.

Rationale:

Nodes might contain **systems** or **applications** that are in the **Sustainment** lifecycle phase. These **Components** are often referred to as **legacy** systems or applications. If a Node needs to expose functionality or data from the legacy Component, changing the internals of such Components to support net-centricity is often impractical with little return on investment. This design pattern offers a reasonable interim solution.

Referenced By:

[Integration of Legacy Systems](#)
[Design Tenet: Open Architecture](#)
[Design Tenet: Service-Oriented Architecture \(SOA\)](#)
[Interoperability](#)

Evaluation Criteria:

1) Test: [G1581.1]

Does the Node use **facade design patterns** such as the wrapper or adapter pattern to expose the functionality of legacy systems or applications?

Procedure:

Make sure that all the Components that are exposed to the internal Node Components or to the external network (with the Node as a proxy) use a facade design pattern such as wrapper or adapter.

Example:

None.

G1582

Statement:

In Node **Enterprise Service** schedules, include version numbers of standard Enterprise Services interfaces being implemented.

Rationale:

Given the complexity, varied implementation timing, and leading edge nature of **Enterprise Services**, the **orchestration** of efforts is essential for the successful integration of the Node's Components. The dependencies captured by such a schedule should clearly show what capabilities will be available and when during the Node's lifecycle.

Referenced By:

[Design Tenet: Network Connectivity Maintainability Coordination of Node and Enterprise Services](#)

Evaluation Criteria:

1) Test: [G1582.1]

Are Enterprise Services interface versions provided on the enterprise service schedule for the Node?

Procedure:

Review the Enterprise Services schedule published for the Node and make sure the schedule provides necessary details including specific version numbers, workarounds, assumptions, constraints and configuration limitations that are interwoven into the schedule.

Example:

An Enterprise Service might be releasing a new version during the lifecycle of the Node's development; which version's functionality will be available when is essential for the successful integration of the Node's Components.

2) Test: [G1582.2]

Are Enterprise Services interface versions provided on the enterprise service schedule for the Component?

Procedure:

Review the Enterprise Services schedule published for the Component and make sure the schedule provides necessary details including specific version numbers, workarounds, assumptions, constraints and configuration limitations that are interwoven into the schedule.

Example:

An Enterprise Service might be releasing a new version during the lifecycle of the Node's development; which version's functionality will be available when is essential so the Component can utilize the appropriate available capabilities.

G1583

Statement:

Provide routine **Enterprise Services** schedule updates to every **Component** of a Node.

Rationale:

A fundamental justification for the existence of nodes is to ensure it provides a shared infrastructure for its Components. If that infrastructure evolves independently of the Components, then they may be developed at timeframes and rates of evolution that differ from the capabilities of the available shared infrastructure. In addition, Components may be members of multiple Nodes, providing an additional coordination challenge. Regular updates to the Components of the master schedule will assist in managing this challenge.

Referenced By:

Maintainability
Coordination of Internal Components

Evaluation Criteria:

1) Test: [G1583.1]

Are there multiple iterations of the Enterprise Services schedule developed over time and is the most recent update timely?

Procedure:

Check for version numbering and release dates of the Enterprise Services schedule. Ensure that a reasonably recent update is available.

Example:

None.

G1584

Statement:

Provide a transport infrastructure that is shared among **Components** within the Node.

Rationale:

Transport elements provided by the Node are a means for the Node to implement **Global Information Grid (GIG) Information Assurance (IA)** boundary protections, bind Components together, and satisfy other enterprise requirements. As transport elements are an essential piece of the net-centric puzzle, they also play a key role in minimizing interoperability issues. A Node's provisioning of the shared transport and related guidance is a key aspect of its existence.

Referenced By:

[Design Tenet: Transport Goal Node Transport](#)

Evaluation Criteria:

1) Test: [G1584.1]

Does the Node's design provide for a transport infrastructure?

Procedure:

Review the Node's infrastructure design and ensure that the Node provides the necessary transport elements for shared use by its Components.

Example:

None.

2) Test: [G1584.2]

Are the Node's Components using the Node provisioned transport infrastructure?

Procedure:

Review the design of the Node's Components (see [G1569](#)) and ensure that they all utilize the common transport infrastructure of inter-Nodal communication.

Example:

None.

G1585

Statement:

Provide a transport infrastructure for the Node that implements **Global Information Grid (GIG) Information Assurance (IA)** boundary protections.

Rationale:

The **Global Information Grid (GIG)** is intended to be the **outside world** for all the Components within the Node. In order to protect the Components within the Node from the outside world and to protect the outside world from the Node, the Node should control the **IA** Boundary.

Referenced By:

Node Transport
Design Tenet: Net-Centric IA Posture and Continuity of Operations
Design Tenet: Transport Goal

Evaluation Criteria:

1) Test: [G1585.1]

Is there an IA device in the acquisition list?

Procedure:

L

Look for an IA device within the parts list for the Node.

Example:

None.

2) Test: [G1585.2]

Is the IA device configured to meet security requirements?

Procedure:

Check the Node's IA installation guide and look for procedures that describe how to configure the IA device for the Node's particular needs.

Example:

None.

G1586

Statement:

Provide a transport infrastructure for the Node that is **Internet Protocol Version 6** (IPv6) capable in accordance with the appropriate governing transition plan.

Rationale:

During the transition period in the DoD community (FY06-FY15) networks, services and applications will be in a mixed environment. All Critical **Key Performance Parameters** (KPPs) must be able to operate in an **Internet Protocol Version 4** (IPv4) only network, an **Internet Protocol Version 6** (IPv6) only network, and a dual-stack network.

Referenced By:

Design Tenet: IPv6
Design Tenet: Transport Goal
IPv4 to IPv6 Transition

Evaluation Criteria:

1) **Test:** [G1586.1]

Does the system operate in an Internet Protocol Version 6 (IPv6) only Network?

Procedure:

Critical Functions will be tested in a Network that only supports Internet Protocol Version 6 (IPv6). The host must be able to complete all critical functions utilizing only IPv6 on the network (no tunneling).

Example:

None.

G1587

Statement:

Prepare an **Internet Protocol Version 6** (IPv6) transition plan for the Node.

Rationale:

The transition from **Internet Protocol Version 4** (IPv4) to **Internet Protocol Version 6** (IPv6) is non-trivial and requires a great deal of coordination and effort on the part of everyone involved. The transition plan helps to minimize the potential disastrous side effects of the transition.

Referenced By:

[IPv4 to IPv6 Transition](#)
[Design Tenet: IPv6](#)

Evaluation Criteria:

1) **Test:** [G1587.1]

Is there an Internet Protocol Version 6 (IPv6) transition plan for the Node?

Procedure:

Look for an Internet Protocol Version 6 (IPv6) transition plan document.

Example:

None.

G1588

Statement:

Coordinate an **Internet Protocol Version 6** (IPv6) transition plan for a Node with the **Components** that comprise the Node.

Rationale:

The effects of the transition from **Internet Protocol Version 4** (IPv4) to **Internet Protocol Version 6** (IPv6) is isolated in the Node infrastructure but can have impacts on all the **Components** that comprise the Node. The transition Plan should cover a "window" that allows all the Components to operate in either IPv4 or IPv6 (i.e., **Dual Stack Mode**) to make the transition.

Referenced By:

[IPv4 to IPv6 Transition Design Tenet: IPv6](#)

Evaluation Criteria:

1) **Test:** [G1588.1]

Does the plan allow for a **Dual Stack** environment at least during some transition period?

Procedure:

Look for a part of the transition plan that addresses **Dual Stack** mode of operation.

Example:

None.

G1589

Statement:

Address issues in the appropriate governing **IPv6** transition plan as part of the Internet Protocol Version 6 (IPv6) Transition Plan for a Node.

Rationale:

DoD has mandated that each service create an **IPv6** transformation office to manage the transition to IPv6. Node transition plans must be aligned and in conformance with the appropriate governing office's plans or criteria.

Referenced By:

[IPv4 to IPv6 Transition Design Tenet: IPv6](#)

Evaluation Criteria:

1) Test: [G1589.1]

Does the Node's IPv6 Transition Plan have a section that addresses specific criteria established by the appropriate governing IPv6 transition office or plan?

Procedure:

Review the IPv6 plan for a section or specific criteria that address the appropriate items from the appropriate governing plan or is approved by the appropriate governing office.

Example:

The Air Force IPv6 Transition Office requires each program to develop a plan with approval by the transition office (in lieu of aligning with a central plan). To check an Air Force Node's alignment, look to see that the Node's IPv6 transition plan is approved by the appropriate authority.

G1590

Statement:

Include transition of all the impacted elements of the network as part of the **Internet Protocol Version 6** (IPv6) Transition Plan for a Node.

Rationale:

Internet Protocol Version 6 (IPv6) transition has an impact on many transport infrastructure **Components**. The Node's IPv6 Transition Plan should include transition of all impacted network elements including **DNS**, routing, security, and dynamic address assignment. The DoD IPv6 Network Engineer's Guidebook (Draft) and the DoD IPv6 Application Engineer's Guidebook (Draft) provide guidance for transition of impacted Components.

Referenced By:

[IPv4 to IPv6 Transition Design Tenet: IPv6](#)

Evaluation Criteria:

1) Test: [G1590.1]

Does the Internet Protocol Version 6 (IPv6) Transition Plan address the impact of the transition to IPv6 on the Domain Name Service (DNS)?

Procedure:

Review the plan and look for a section dedicated to the Domain Name Service (DNS). At a minimum, it should indicate that there is no impact.

Example:

None.

2) Test: [G1590.2]

Does the Internet Protocol Version 6 (IPv6) Transition Plan address the impact of the transition to IPv6 on routing?

Procedure:

Review the plan and look for a section dedicated to routing. At a minimum, it should indicate that there is no impact.

Example:

None.

3) Test: [G1590.3]

Does the Internet Protocol Version 6 (IPv6) Transition Plan address the impact of the transition to IPv6 on security?

Procedure:

Review the plan and look for a section dedicated to security. At a minimum, it should indicate that there is no impact.

Example:

None.

4) Test: [G1590.4]

Does the Internet Protocol Version 6 (IPv6) Transition Plan address the impact of the transition to IPv6 on dynamic address assignment?

Procedure:

Review the plan and look for a section dedicated to dynamic address assignment. At a minimum, it should indicate that there is no impact.

Example:

None.

G1591

Statement:

Prepare **IPv6** Working Group products as part of the Internet Protocol Version 6 (IPv6) transition plan for a Node.

Rationale:

The **Internet Protocol Version 6** (IPv6) Working Group has prescribed various products that can aid in the planning for the transition from **Internet Protocol Version 4** (IPv4) to IPv6. The Node's Transition Plan should prepare these products to ensure that all the required activities are addressed.

Referenced By:

[IPv4 to IPv6 Transition Design Tenet: IPv6](#)

Evaluation Criteria:

1) **Test:** [G1591.1]

Are the Internet Protocol Version 6 (IPv6) Working Group products in the Node's Transition Plan?

Procedure:

Look for the Working Group products in the Node's Transition Plan.

Example:

None.

G1592

Statement:

Include interoperability testing in the plan as part of the **Internet Protocol Version 6 (IPv6)** transition plan for a Node.

Rationale:

During the **DoD** transition period, a mixed **IPv4/IPv6** environment will exist. Interoperability testing with both standards will ensure the Node can fully function during the transition period with all other Nodes.

Referenced By:

Design Tenet: IPv6
IPv4 to IPv6 Transition

Evaluation Criteria:

1) **Test:** [G1592.1]

Does the Node's IPv6 transition plan address interoperability testing in a mixed environment?

Procedure:

Review the transition plan and verify that a test plan exists that specifically addresses interoperability testing in a mixed IP environment.

Example:

None.

G1595

Statement:

Implement **Domain Name System** (DNS) to manage hostname/address resolution within the Node.

Rationale:

Using **Domain Name System** (DNS) obviates the need for hard-coding **Internet Protocol** (IP) addresses within the Node. In addition, DNS servers local to the Node allow for stable access of replicated entries from outside the Node.

Referenced By:

[Domain Name System \(DNS\)](#)
[Design Tenet: Packet Switched Infrastructure](#)
[Design Tenet: IPv6](#)

Evaluation Criteria:

1) Test: [G1595.2]

Are there any hard coded Internet Protocol (IP) addresses within the source code or data files?

Procedure:

Look at the source code, properties files and descriptor files for the occurrence of Internet Protocol Version 4 (IPv4) or Internet Protocol Version 6 (IPv6) Internet Protocol (IP) addresses.

Example:

None.

2) Test: [G1595.1]

Is there a Domain Name System (DNS) server in the Node acquisition list?

Procedure:

Look for a Domain Name System (DNS) server within the parts list for the Node.

Example:

None.

G1596

Statement:

Use **Domain Name System (DNS) Mail eXchange (MX) Record** capabilities to configure electronic mail delivery to the Node.

Rationale:

Utilizing the **Domain Name System (DNS) Mail eXchange (MX) record** capability will avoid the need to hard code delivery routes and instructions within a Node's email system and buffers it from physical changes made to email delivery points and routes outside of the Node. The DNS MX record is a standard and commonly accepted mechanism for resolving email delivery routes and addresses across the Internet.

Internet Engineering Task Force (IETF) Request for Comments (RFC) [2821](#) of April 2001 established rules for MX record usage.

Referenced By:

[Domain Name System \(DNS\)](#)
[Design Tenet: Packet Switched Infrastructure](#)

Evaluation Criteria:

1) Test: [G1596.1]

Are there **Mail eXchange (MX) Records** defined within the **Domain Name System (DNS)**?

Procedure:

Look at the Domain Name System (DNS) records for Mail eXchange (MX) Records.

Example:

None.

G1598

Statement:

Allow dynamic **Domain Name System** (DNS) updates to the Node's internal DNS service by local **Dynamic Host Configuration Protocol** (DHCP) **server(s)**.

Rationale:

There are two basic methods for assigning of **Internet Protocol** (IP) addresses within a network: static and dynamic. Static addresses are assigned to a particular system and never change. Dynamic Internet Protocol (IP) addresses are issued for a variable length of time: the **DCHP lease time**. **Dynamic Host Configuration Protocol** (DHCP) is the principle mechanism used to assign and manage dynamic IP addresses. If the DHCP servers are allowed to update the **Domain Name System** (DNS), then the number of static addresses required by the system can be drastically reduced with preference being given to requesting services by domain name rather than IP address.

Referenced By:

[Design Tenet: Packet Switched Infrastructure Domain Name System \(DNS\)](#)

Evaluation Criteria:

1) Test: [G1598.1]

Does the Domain Name System (DNS) server in the Node acquisition list support updates from Dynamic Host Configuration Protocol (DHCP) Servers?

Procedure:

Review the Domain Name System (DNS) server specification to confirm that it supports such operations.

Example:

None.

G1599

Statement:

Support both **Internet Protocol Version 4** (IPv4) and **Internet Protocol Version 6** (IPv6) simultaneously in the Node's **Domain Name System** (DNS) service.

Rationale:

During the transition period in the DoD community (FY06-FY15) networks, services and applications will be in a mixed environment. The Domain Name System (DNS) returns different address records depending on the Internet Protocol (IP) environment: A records for IPv4 or AAAA records for IPv6. A DNS must be able to support both.

Referenced By:

[IPv4 to IPv6 Transition
Domain Name System \(DNS\)
Design Tenet: IPv6](#)

Evaluation Criteria:

1) **Test:** [G1599.1]

Does the Domain Name System (DNS) server support both A and AAAA records?

Procedure:

Review the Domain Name System (DNS) specification to confirm that it supports both A and AAAA records.

Example:

None.

G1600

Statement:

Obtain from DISA any and all **Internet Protocol Version 6** (IPv6) addresses used on DoD systems in the Node.

Rationale:

All the **Internet Protocol** (IP) addresses in use on a DoD network must be from an appropriate clearing house in order to maintain control and accountability on the network. **DISA** is the clearing house for all DoD addresses.

Referenced By:

IPv4 to IPv6 Transition
Domain Name System (DNS)
Design Tenet: IPv6

Evaluation Criteria:

1) Test: [G1600.1]

Is there a proper entry in the Military Network Information Center (MILNIC) for every IP address assigned to the system?

Procedure:

Verify an adequate address allocation has been made in Military Network Information Center (MILNIC) for the system.

Example:

None.

G1601

Statement:

Use configurable **routers** to provide dynamic **Internet Protocol** (IP) address management using **Dynamic Host Configuration Protocol** (DHCP).

Rationale:

There are two basic methods for assigning of **Internet Protocol** (IP) addresses within a network: static and dynamic. Static addresses are assigned to a particular system and never change. Dynamic IP addresses are issued for a variable length of time: the **DCHP lease time**. **Dynamic Host Configuration Protocol** (DHCP) is the principle mechanism used to assign and manage dynamic IP addresses.

Referenced By:

[Design Tenet: Inter-Network Connectivity Routers](#)
[Design Tenet: Network Connectivity Multicast](#)
[Design Tenet: Packet Switched Infrastructure](#)

Evaluation Criteria:

1) **Test:** [G1601.1]

Does the router in the Node acquisition list support Dynamic Host Configuration Protocol (DHCP)?

Procedure:

Review the router specification to confirm that it supports such operations.

Example:

None.

G1602

Statement:

Use configurable **routers** to provide static **Internet Protocol** (IP) addresses.

Rationale:

Some network **Components** such as the **routers** themselves and other security related services must reside on static **Internet Protocol** (IP) addresses. Serious compromises in the network can arise if these services are allowed to be dynamic.

Referenced By:

[Design Tenet: Inter-Network Connectivity Routers](#)
[Design Tenet: Network Connectivity](#)
[Design Tenet: Packet Switched Infrastructure](#)

Evaluation Criteria:

1) **Test:** [G1602.1]

Does the **router** in the Node acquisition list support static **Internet Protocol** (IP) addressing?

Procedure:

Review the router specification to confirm that it supports such operations.

Example:

None.

G1604

Statement:

Use configurable **routers** to provide time synchronization services using **Network Time Protocol** (NTP).

Rationale:

Over time, most computer clocks drift. **Network Time Protocol** (NTP) is one way to ensure that a computer clock stays accurate. Unfortunately, in order to stay synchronized, a network connection needs to be maintained. In environments that have limited bandwidth or poor **quality of service** (QoS) this can become a major issue.

Referenced By:

[Time Services](#)
[Design Tenet: Inter-Network Connectivity](#)
[Design Tenet: Packet Switched Infrastructure](#)
[Routers](#)
[Design Tenet: Network Connectivity](#)

Evaluation Criteria:

1) **Test:** [G1604.1]

Does the **router** in the Node acquisition list support NTP Service?

Procedure:

Review the routers specification to confirm that it supports such operations.

Example:

None.

G1605

Statement:

Use configurable **routers** to provide **multicast** addressing.

Rationale:

Multicast addresses identify interfaces that allow a packet to be sent to all the addresses registered for the multicast service. This allows network to easily support applications such as **collaboration**, audio and video.

Referenced By:

[Routers](#)
[Design Tenet: Network Connectivity](#)
[Design Tenet: Packet Switched Infrastructure](#)
[Design Tenet: Inter-Network Connectivity](#)

Evaluation Criteria:

1) Test: [G1605.1]

Does the **router** in the Node acquisition list support NTP Service?

Procedure:

Review the router specification to confirm that it supports such operations.

Example:

None.

G1606

Statement:

Manage **routers** remotely from within the **Node**.

Rationale:

Router manufactures routinely provide tools to enable remote configuration and management of the router. These tools can speed and centralize the administration of the Nodes routers.

Referenced By:

[Design Tenet: Inter-Network Connectivity Routers](#)
[Design Tenet: Network Connectivity](#)
[Design Tenet: Decentralized Operations and Management](#)
[Design Tenet: Packet Switched Infrastructure](#)

Evaluation Criteria:

1) Test: [G1606.1]

Does the **router** in the Node acquisition list support remote management?

Procedure:

Review the router specification to confirm that it supports such operations.

Example:

None.

G1607

Statement:

Configure routers according to **National Security Agency** (NSA) [Router Security Configuration](#) guidance.

Rationale:

The *Router Security Configuration Guide* provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of **Internet Protocol** (IP) routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network **Components**, and help protect the integrity and confidentiality of network traffic.

Referenced By:

[Design Tenet: Packet Switched Infrastructure](#)
[Design Tenet: Inter-Network Connectivity](#)
[Design Tenet: Concurrent Transport of Information Flows](#)
[Routers](#)
[Design Tenet: Network Connectivity](#)
[Design Tenet: Encryption and HAIPE](#)

Evaluation Criteria:

1) Test: [G1607.1]

Is the **Router** Security Checklist complete and up to date?

Procedure:

Check for the occurrence of the checklist; there should be a copy for every time the checklist has been completed. The checklist should indicate the date, time and results of the checklist with recommendation actions.

Example:

Router Security Checklist

This security checklist is designed to help review router security configuration and remind a user of any security areas that might be missed.

- Router security policy written, approved, distributed.
- Router IOS version checked and up to date.
- Router configuration kept off-line, backed up, access to it limited.
- Router configuration is well-documented, commented.
- Router users and passwords configured and maintained.
- Password encryption in use, enable secret in use.
- Enable secret difficult to guess, knowledge of it strictly limited. (if not, change the enable secret immediately)
- Access restrictions imposed on Console, Aux, VTYs.

Part 4: Node Guidance

- Unneeded network servers and facilities disabled.
- Necessary network services configured correctly (e.g. DNS)
- Unused interfaces and VTYs shut down or disabled.
- Risky interface services disabled.
- Port and protocol needs of the network identified and checked.
- Access lists limit traffic to identified ports and protocols.
- Access lists block reserved and inappropriate addresses.
- Static routes configured where necessary.
- Routing protocols configured to use integrity mechanisms.
- Logging enabled and log recipient hosts identified and configured.
- Router's time of day set accurately, maintained with NTP.
- Logging set to include consistent time information.
- Logs checked, reviewed, archived in accordance with local policy.
- SNMP disabled or enabled with good community strings and ACLs.

G1608

Statement:

Obtain the reference time for the Node time service from a globally synchronized time source.

Rationale:

Currently Network Time Service is not a ubiquitous service across the **Global Information Grid** (GIG). Security directives prevent IP-based time synchronization across **firewall** boundaries (e.g., AFI 33-115, 16). An example of a precise globally synchronized time source is a **Global Positioning System** (GPS) system.

Referenced By:

[Design Tenet: Packet Switched Infrastructure Time Services](#)
[Design Tenet: Inter-Network Connectivity](#)
[Design Tenet: Network Connectivity](#)

Evaluation Criteria:

1) **Test:** [G1608.1]

Does the Node acquisition list include a precise globally synchronized time source such as **Global Positioning System** (GPS) system?

Procedure:

Review the acquisition list for a precise globally synchronized time source such as a **Global Positioning System** (GPS) system that can be used to accurately synchronize time.

Example:

None.

G1609

Statement:

Arrange for a backup time source for the Node time service.

Rationale:

The most common type of backup time sources are crystal oscillators. The physical characteristics of the piezoelectric quartz crystal produce electrical oscillations at an extremely accurate frequency. This frequency can be used to mark time.

Referenced By:

[Design Tenet: Network Connectivity](#)
[Design Tenet: Packet Switched Infrastructure](#)
[Design Tenet: Inter-Network Connectivity](#)
[Time Services](#)

Evaluation Criteria:

1) Test: [G1609.1]

Does the Node acquisition list include a backup time system?

Procedure:

Review the acquisition list for a backup time system that can be used to synchronize time accurately. For example: crystal oscillator, cesium or rubidium crystal oscillators. Crystal oscillator types and their abbreviations:

MCXO	microcomputer-compensated crystal oscillator
OCVCXO	oven-controlled voltage-controlled crystal oscillator
OCXO	oven-controlled crystal oscillator
RbXO	rubidium crystal oscillators (RbXO)
TCVCXO	temperature-compensated-voltage controlled crystal oscillator
TCXO	temperature-compensated crystal oscillator
VCXO	voltage-controlled crystal oscillator

Example:

None.

G1610

Statement:

Configure the **Dynamic Host Configuration Protocol** (DHCP) services to assign **multicast** addresses.

Rationale:

When **Dynamic Host Configuration Protocol** (DHCP) services assign temporary **Internet Protocol** (IP) addresses to clients, the clients may wish to participate in a **multicast** service. Therefore, the DHCP service must support the assignment of multicast addresses as part of normal operations.

Referenced By:

Design Tenet: Network Connectivity
Multicast
Design Tenet: Packet Switched Infrastructure
Design Tenet: Inter-Network Connectivity

Evaluation Criteria:

1) Test: [G1610.1]

Does the **router** in the Node acquisition list support the assignment of **multicast** Internet Protocol (**IP**) addresses as part of the normal **Dynamic Host Configuration Protocol** (DHCP) service?

Procedure:

Review the **router** specification to confirm that it supports such operations.

Example:

None.

G1611

Statement:

Implement Internet Protocol (**IP**) gateways to interoperate with the **Global Information Grid** (GIG) until IP is supported natively for **Components** that are not IP networked, such as aircraft data links (**Link-16**, **SADL**, etc.).

Rationale:

Component systems such as aircraft data links (Link-16, SADL, etc), should implement **Transmission Control Protocol/Internet Protocol** (TCP/IP) gateways to interoperate with the **Global Information Grid** (GIG) until TCP/IP is supported natively. This acts as an interim step that can be used to bridge the **Internet Protocol** (IP) divide.

Referenced By:

Design Tenet: Packet Switched Infrastructure
Integration of Non-IP Transports

Evaluation Criteria:

1) Test: [G1611.1]

Is there an Internet Protocol (IP) gateway in the system?

Procedure:

Identify **Transmission Control Protocol/Internet Protocol** (TCP/IP), **User Datagram Protocol** (UDP) or **DDS** code that will be front-ended by a gateway.

Example:

None.

G1612

Statement:

Implement Internet Protocol (**IP**) gateways as a **service**.

Rationale:

This does not mean that the service is a **Web service** or that it is limited to request/reply or other such usage patterns. In fact, for high-frequency data, such as track reporting, a function of the service could be to set up an out-of-band communication with a subscriber.

Referenced By:

[Integration of Non-IP Transports](#)
[Design Tenet: Packet Switched Infrastructure](#)

Evaluation Criteria:

1) **Test:** [G1612.1]

Is the gateway developed as a service that could be advertised in a registry?

Procedure:

Examine the gateway and determine if it is a service.

Example:

None.

G1613

Statement:

Prepare a **Node** to host new **Component** services developed by other Nodes or by the **enterprise** itself.

Rationale:

A key aspect of an open systems approach to interoperability is **modular design** which is also a basic tenet of good development practice. Modularity will support the dynamic redeployment of a **Component** into different Nodes that requires the capabilities of the Component thus promoting broader interoperability between different Nodes and Components. Where possible, Nodes should adopt standards based, platform independent frameworks that facilitate **pluggable** deployment capabilities for Components so it can leverage the capabilities developed elsewhere.

Referenced By:

[Cross-Domain Interoperation](#)
[Design Tenet: Cross-Security-Domains Exchange](#)
[Web Client Platform](#)

Evaluation Criteria:

1) **Test:** [G1613.1]

Does the Node support the elements of a modern component based framework such as **Java Platform, Enterprise Edition** (Java EE), **.NET** or **CORBA**?

Procedure:

Look for the existence of Java Platform, Enterprise Edition (Java EE), .NET or CORBA frameworks with in the Node's Component list or in its delivered software.

Example:

None.

G1619

Statement:

Configure **clients** with a **Common Access Card (CAC)** reader.

Rationale:

DoD Instruction 8520.2, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling* [R1206], defines **Common Access Card (CAC)** applicability and scope, in part, as follows:

This Instruction applies to:... 2.4. All DoD unclassified and classified information systems including networks (e.g., Non-secure Internet Protocol (IP) Router Network, Secret Internet Protocol Router Network, Web servers, and e-mail systems. Excluded are Sensitive Compartmented Information, and information systems operated within the Department of Defense that fall under the authority of the Director of Central Intelligence Directive (DCID) 6/3 (reference (h)).

Referenced By:

[Design Tenet: Identity Management, Authentication, and Privileges
Common Access Card \(CAC\) Reader](#)

Evaluation Criteria:

1) Test: [G1619.1]

Do all the **client** and **server** hardware come equipped with **Common Access Card (CAC)** Readers?

Procedure:

Review the hardware list and verify that all hardware comes with or has external CAC readers.

Example:

None.

G1621

Statement:

Provide a Node Web infrastructure for all **Components** within the Node.

Rationale:

A Web application infrastructure includes those elements which allow an application developer to deploy an application at a Node without regard to how the application will display results to an end user, execute or be deployed. By providing open access to a common Web infrastructure, Components are relieved of having to implement their own divergent Web infrastructure, thereby promoting increased interoperability and reusability.

Referenced By:

[Web Infrastructure](#)

Evaluation Criteria:

1) Test: [G1621.1]

Does the Node acquisition list include duplicate Web application infrastructure elements that are not provided by the Node?

Procedure:

Review the acquisition list for Web application infrastructure elements (Web Portal, Web Server and Web Application Containers). If duplicates are found or not provided by Node, address the issue with the appropriate stakeholders.

Example:

None.

G1622

Statement:

Implement **commercial off-the-shelf** (COTS) software that protects against malicious code on each operating system in the Node in accordance with the Desktop Application **Security Technical Implementation Guide** (STIG).

Rationale:

The viral and worm assault on computing resources is major concern but is not strictly limited to DoD hardware and operating systems. It has become a ubiquitous, wide spread problem that spreads destruction indiscriminately. Since the problem is not strictly a DoD problem, **commercial off-the-shelf** (COTS) solutions are always being updated to meet the current threats and are essential in protecting the assets. All hardware platforms should employ virus and worm detection and removal software that is routinely run (especially on hardware the runs Microsoft products).

Note: For purposes of this guidance, anti virus software includes related update and maintenance capabilities typically available with such packages.

Referenced By:

[Host Information Assurance](#)
[Other Design Tenets](#)

Evaluation Criteria:

1) Test: [G1622.1]

Do all hardware devices listed in the Node acquisition list have COTS licensed virus and worm detection software?

Procedure:

Review the Node acquisition list and make sure there is one license for each piece of computer hardware.

Example:

None.

2) Test: [G1622.2]

Do all hardware devices listed in the Node acquisition list have COTS virus and worm detection software installed?

Procedure:

Review the prerequisites in the installation manual for virus and worm software.

Example:

None.

G1623

Statement:

Implement personal **firewall** software on **client** or **server** hardware used for remote connectivity in accordance with the Desktop Applications, Network and Enclave **Security Technical Implementation Guides (STIGs)**.

Rationale:

All hardware that is plugged into a network is subject to attack by hackers. In addition to hardware **firewalls**, every piece of hardware should be protected by a software firewall. These firewalls continuously monitor the activity on the network port and detect possible hostile attacks. The user has the discretion to block hostile attacks permanently or for a particular occasion. Since this problem is not restricted to DoD assets, **Commercial off-the-shelf (COTS)** products are continuously being updated to meet the latest threats and are essential in meeting these threats.

Referenced By:

[Host Information Assurance](#)
[Other Design Tenets](#)
[Design Tenet: Decentralized Operations and Management](#)
[Design Tenet: Inter-Network Connectivity](#)

Evaluation Criteria:

1) Test: [G1623.1]

Do all the hardware devices listed in the Node acquisition list have COTS software firewall licensed software?

Procedure:

Review the Node acquisition list and make sure there is one license for each piece of computer hardware.

Example:

None.

2) Test: [G1623.2]

Do all hardware devices listed in the Node acquisition list have COTS **firewall** software installed and is it enabled?

Procedure:

Review the prerequisites in the installation manual for firewall software.

Example:

None.

G1624

Statement:

Install anti-**spyware** on all **client** and **server** hardware.

Rationale:

Spyware is a category of malicious software that can impact a system's operation in ways similar to virus and other intrusions. Extending the principles of protection against viruses and other intrusions to spyware is an essential activity to ensure stable system operation and security.

Referenced By:

[Other Design Tenets](#)
[Host Information Assurance](#)

Evaluation Criteria:

1) Test: [G1624.1]

Do all the hardware devices listed in the Node acquisition list have COTS software anti-spyware licensed software?

Procedure:

Review the Node acquisition list and make sure there is one license for each piece of computer hardware.

Example:

None.

2) Test: [G1624.2]

Do all hardware devices listed in the Node acquisition list have COTS anti-spyware software installed and is it enabled?

Procedure:

Review the prerequisites in the installation manual for firewall software.

Example:

None.

G1625

Statement:

Provide a **commercial off-the-shelf** Directory Service that all of the **Components** of a Node can use.

Rationale:

A Directory Service is a service that stores information about objects on a computer network. Common objects stored by a Directory Service include network users, common resources (such as shares and printers), authentication and authorization information.

Note: *This guidance is provisional pending completion of detailed review.*

Referenced By:

[Directory Services](#)

Evaluation Criteria:

1) Test: [G1625.2]

Is an Open Source directory service going to be used?

Procedure:

Review the prerequisites in the installation manual for open source directory service software.

Example:

None.

2) Test: [G1625.1]

Is there a COTS directory service listed in the Node acquisition list?

Procedure:

Review the Node acquisition list and make sure there is one license for a directory service.

Example:

None.

G1626

Statement:

Identify which **Core Enterprise Services** (CES) capabilities the Node **Components** require.

Rationale:

A Node needs to determine the set of **Core Enterprise Services** (CES) its **Components** will require in order to ensure efficient prioritization of activities and resources to provide those services. NCES has defined a set of common capabilities that help categorize types of services that may be required by a Node's Components. Identification of the capabilities required by Components will help the Node determine which Services will need to be implemented.

Referenced By:

[Design Tenet: Open Architecture
CES Definitions and Status](#)

Evaluation Criteria:

1) **Test:** [G1626.1]

Does the list of Components that comprise the Node indicate which CES capabilities are required to deploy each Component?

Procedure:

Review the list of Components and verify that they have indicated which CES capabilities are required to support the Component.

Example:

None.

G1627

Statement:

Identify the priority of each **Core Enterprise Services** (CES) capability the Node **Components** require.

Rationale:

Identifying the priority of capabilities required by the Node's **Components** will assist the Node in allocation of scarce resources towards the delivery of CES in the Node and minimize risks during deployment of Components within the Node. Some capabilities are **essential** at getting a Component Deployed at a Node. Some are essential for a particular Component increment. With this information the Node can construct a schedule that supports the transition and evolution of the current federation of systems to the **Global Information Grid** (GIG) vision.

Referenced By:

[Design Tenet: Open Architecture](#)
[CES Parallel Development](#)
[CES Definitions and Status](#)

Evaluation Criteria:

1) Test: [G1627.1]

Does the list of Components that comprise the Node indicate the priority of the CES capabilities either relative to each other or as of a date?

Procedure:

Review the list of Components and verify that they have indicated what the priority of the CES capabilities either relative to each other or as of a date.

Example:

None.

G1629

Statement:

Identify which **Net-Centric Enterprise Services** (NCES) capabilities the Node requires during deployment.

Rationale:

Relying on a high-bandwidth **Transmission Control Protocol/Internet Protocol** (TCP/IP) network connection is not a reality for many deployed Nodes. These Nodes will have to develop many of their own CES capabilities for use by their member **Components** while deployed. When the Node is not deployed, it may rely on proxies to the **Net-Centric Enterprise Services** (NCES) services.

Referenced By:

[CES Definitions and Status](#)
[Design Tenet: Joint Net-Centric Capabilities](#)
[Design Tenet: Open Architecture](#)

Evaluation Criteria:

1) Test: [G1629.1]

Does the Node have a list of **Net-Centric Enterprise Services** (NCES) capabilities that it depends on while deployed?

Procedure:

Review the Node's documents for a list of Net-Centric Enterprise Services (NCES) capabilities required by the Node while deployed.

Example:

None.

G1630

Statement:

Comply with the applicable **Global Information Grid (GIG) Key Interface Profiles (KIPs)** for implemented **Core Enterprise Services (CES)** in the Node.

Rationale:

When a **CES** is implemented locally, use the **Global Information Grid (GIG) Key Interface Profiles (KIPs)** developed by **DISA** as the authoritative definition of the interfaces. This allows a **Component** that is hosted by one Node to be hosted on another Node with a minimal impact.

Referenced By:

Design Tenet: Open Architecture
CES and Intermittent Availability
Key Interface Profile (KIP)

Evaluation Criteria:

1) Test: [G1630.1]

Do all **CES** used locally within the Node implement the applicable **Global Information Grid (GIG) Key Interface Profile (KIP)**?

Procedure:

Verify that the interfaces for Core Enterprise Services (CES) implement Global Information Grid (GIG) Key Interface Profiles (KIPs) for that CES.

Example:

None.

G1631

Statement:

Expose **Core Enterprise Services** (CES) that comply with the applicable **Global Information Grid** (GIG) **Key Interface Profiles** (KIPs) in all Node services **proxies**.

Rationale:

A Node may expose or control access to **Global Information Grid** (GIG) **CES** by using **proxies**. This allows a **Component** that is hosted by one Node to be hosted on another Node with a minimal impact.

Referenced By:

[Design Tenet: Open Architecture](#)
[Key Interface Profile \(KIP\)](#)
[CES and Intermittent Availability](#)

Evaluation Criteria:

1) **Test:** [G1631.1]

Do all **CES proxies** locally defined within the Node expose CES using the applicable **Global Information Grid** (GIG) **Key Interface Profile** (KIP)?

Procedure:

Verify that the interfaces for CES proxies follow Key Interface Profiles (KIPs) for that Global Information Grid (GIG) KIP.

Example:

None.

G1632

Statement:

Certify and accredit Nodes with all applicable DoD **Information Assurance** (IA) processes.

Rationale:

Nodes are part of the DoD **Global Information Grid** (GIG) and are consequently required to have DoD **Information Assurance** (IA) certification and accreditation. Details for certification and accreditation are specified in [DoD Directive 8500.1](#), [DoD Instruction 8500.2](#), [DoD Directive 8580.1](#), and [DoD Instruction 5200.40](#). Satisfaction of these requirements results in IA compliance verification of the Node.

Referenced By:

Other Design Tenets
Information Assurance (IA)
Design Tenet: Net-Centric IA Posture and Continuity of Operations

Evaluation Criteria:

1) Test: [G1632.1]

Does the Node have DoD **Information Assurance** (IA) certification and accreditation?

Procedure:

Ask to examine the certification and accreditation reports.

Example:

None.

G1633

Statement:

Host only DoD **Information Assurance** (IA) certified and accredited **Components**.

Rationale:

Nodes that expose the external Node users to non-certified or non-accredited **Components** represent a risk to the stability of the entire Node network and can introduce interoperability issues between Nodes (and related Components).

Referenced By:

[Information Assurance \(IA\)](#)
[Other Design Tenets](#)
[Design Tenet: Net-Centric IA Posture and Continuity of Operations](#)

Evaluation Criteria:

1) **Test:** [G1633.1]

Does the Node have a plan to scan all Components on a routine basis?

Procedure:

Look for a plan and examine the results of the scan.

Example:

None.

G1634

Statement:

Certify and accredit **Components** with all applicable DoD **Information Assurance** (IA) processes.

Rationale:

Each **Component** could theoretically be deployed on any Node. Therefore, it is the responsibility of the Component to be DoD **Information Assurance** (IA) certified and accredited.

Referenced By:

[Information Assurance \(IA\)](#)
[Design Tenet: Net-Centric IA Posture and Continuity of Operations](#)
[Other Design Tenets](#)

Evaluation Criteria:

1) **Test:** [G1634.1]

Are all the **Components** DoD **Information Assurance** (IA) certified and accredited?

Procedure:

Examine the certification and accreditation reports.

Example:

None.

G1635

Statement:

Make Nodes that will be part of the **Global Information Grid** (GIG) consistent with the *GIG Integrated Architecture*.

Rationale:

The **Global Information Grid** (GIG) architecture describes the basic, high level architecture in which Nodes reside. It is an integrated architecture consisting of the various **DoDAF** views. It provides a common lexicon and defines a basic infrastructure for the performance of information exchanges with other GIG Nodes using the **GIG Enterprise Services** (GES) and the **Net-Centric Enterprise Services** (NCES). The GIG Integrated Architecture is available via the DoD Architecture Repository System (DARS), <https://dars1.army.mil/> [user account and PKI certificate required for access].

Referenced By:

Design Tenet: Service-Oriented Architecture (SOA)
Interoperability
Integrated Architectures

Evaluation Criteria:

1) Test: [G1635.1]

Are there **DoDAF** integrated architecture products defined for the Node that are consistent with the **GIG** Integrated Architecture?

Procedure:

Look for the occurrence of **Operational View** (OV), **Systems and ServicesView** (SV), **Technical Standards View** (TV) and **All Views** (AV).

Example:

None.

G1636

Statement:

Comply with the **Net-Centric Operations and Warfare Reference Model** (NCOW RM).

Rationale:

The **Net-Centric Operations and Warfare Reference Model** (NCOW RM) is focused on achieving net-centricity. Compliance with the NCOW RM translates to articulating how each Node approaches and implements net-centric features. Compliance does not require separate documentation; rather, it requires that a Node address, within existing architecture, analysis, and program architecture documentation, the issues identified by using the model, and further, make explicit the path to net-centricity the program is taking.

Node compliance with the NCOW RM is demonstrated through inspection and analysis:

- Use of NCOW RM definitions and vocabulary;
- Incorporation of NCOW RM Operational View (OV) capabilities and services in the materiel solution;
- Incorporation of NCOW RM Technical View **Information Technology** (IT) and **National Security Systems** (NSS) standards in the Technical View products developed for the materiel solution.

Compliance with the NCOW RM is a critical component of compliance with the **Net-Ready Key Performance Parameter** (NR-KPP).

Referenced By:

[Interoperability](#)
[Design Tenet: Service-Oriented Architecture \(SOA\)](#)
[Net-Centric Operations and Warfare Reference Model \(NCOW RM\)](#)

Evaluation Criteria:

1) Test: [G1636.2]

Have the instructions in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) [3170.01](#) been used to check the Node for Net-Centric Operations and Warfare Reference Model (NCOW RM) compliance?

Procedure:

Check Node documentation.

Example:

2) Test: [G1636.3]

Have the instructions in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) [6212.01](#) been used to check the Node for Net-Centric Operations and Warfare Reference Model (NCOW RM) compliance?

Procedure:

Check Node documentation.

Example:

3) Test: [G1636.1]

Have the instructions in the Defense Acquisition University (DAU) Guidebook [section 7.2.6](#) been used to check the Node for NCOW RM compliance?

Procedure:

Check Node documentation.

Example:

G1637

Statement:

Make Node-implemented **directory services** comply with the directory services **Global Information Grid (GIG) Key Interface Profiles (KIPs)**.

Rationale:

When directory services are implemented locally, use the **Global Information Grid (GIG) KIPs** developed by DISA as the authoritative definition of the interfaces. This allows a **Component** that is hosted by one Node to be hosted on another node with a minimal impact.

Referenced By:

Design Tenet: Service-Oriented Architecture (SOA)
Directory Services
Interoperability

Evaluation Criteria:

1) Test: [G1637.1]

Do all directory services used locally within the Node implement the applicable **Global Information Grid (GIG) Key Interface Profile (KIP)**?

Procedure:

Verify that the interfaces for directory services implement Global Information Grid (GIG) Key Interface Profiles (KIPs) for that directory services.

Example:

None.

G1638

Statement:

Comply with the directory services **Global Information Grid (GIG) Key Interface Profiles (KIPs)** in Node directory services **proxies**.

Rationale:

A Node may expose or control access to **Global Information Grid (GIG)** directory services by using **proxies**. This allows a **Component** that is hosted by one Node to be hosted on another node with a minimal impact.

Referenced By:

Directory Services
Design Tenet: Service-Oriented Architecture (SOA)
Interoperability

Evaluation Criteria:

1) Test: [G1638.1]

Do all directory services **proxies** locally defined within the Node expose directory services using the applicable **Global Information Grid (GIG) Key Interface Profile (KIP)**?

Procedure:

Verify that the interfaces for directory services proxies follow Key Interface Profiles (KIPs) for that Global Information Grid (GIG) KIPs.

Example:

None.

G1639

Statement:

Describe **Components** exposed by the Node as specified by the **Service Definition Framework**

Rationale:

The construction of registry entries is specified by the **Service Definition Framework** (SDF) documented in Net-Centric Implementation Directives (NCIDs) S300. The common Service Definition Framework that serves as the basis for adequately describing the offered **Component** service from both a provider's and consumer's perspective. It describes the contract between the Component service provider and the Component service consumer, and serves as the basis for a **Service Level Agreement** (SLA). The common service definition framework consists of elements that include interface, service level, security and implementation information.

Referenced By:

[Service Discovery](#)
[Design Tenet: Enterprise Service Management](#)

Evaluation Criteria:

1) **Test:** [G1639.1]

Is there a **Service Definition Framework** (SDF) available for each of the Components' Services exposed through the Node?

Procedure:

Look for a Service Definition Framework (SDF) for each Component service exposed through the Node.

Example:

None

G1640

Statement:

Register **Components** exposed by the Node with the **DISA**-hosted registries.

Rationale:

The best way for an exposed Node's **Component** service to be discovered is by being registered in the DISA registry. The DISA registry implementation uses **Universal Description, Discovery, Integration** (UDDI).

Referenced By:

Interoperability
Service Discovery

Evaluation Criteria:

1) **Test:** [G1640.1]

Is the exposed Node's Component's service registered in the DISA **Universal Description, Discovery, Integration** (UDDI) Registry?

Procedure:

Examine the DISA Universal Description, Discovery, Integration (UDDI) Registry and look for the exposed Node's Component's service.

Example:

None.

G1641

Statement:

Comply with the Service Discovery **Global Information Grid** (GIG) **Key Interface Profiles** (KIPs) in Node-implemented **Service Discovery** (SD).

Rationale:

When a **Service Discovery** (SD) is implemented locally, the **Global Information Grid** (GIG) Kips developed by DISA should be used as the authoritative definition of the interfaces. This allows a **Component** that is hosted by one Node to be hosted on another node with a minimal impact.

Referenced By:

Service Discovery
Design Tenet: Service-Oriented Architecture (SOA)
Interoperability

Evaluation Criteria:

1) Test: [G1641.1]

Does the **Service Discovery** (SD) used locally within the Node implement the applicable **Global Information Grid** (GIG) **Key Interface Profile** (KIP)?

Procedure:

Verify that the interfaces for Service Discovery (SD) implement Global Information Grid (GIG) Key Interface Profiles (KIPs) for that Service Discovery.

Example:

None.

G1642

Statement:

Comply with the **Service Discovery Global Information Grid (GIG) Key Interface Profiles (KIPs)** in Node Service Discovery (SD) **proxies**.

Rationale:

A Node may expose or control access to **Global Information Grid (GIG) Service Discovery (SD)** by using **proxies**. This allows a **Component** that is hosted by one Node to be hosted on another node with a minimal impact.

Referenced By:

Design Tenet: Service-Oriented Architecture (SOA)
Service Discovery
Interoperability

Evaluation Criteria:

1) Test: [G1642.1]

Do the **Service Discovery (SD) proxies** locally defined within the Node expose Service Discovery using the applicable **Global Information Grid (GIG) Key Interface Profile (KIP)**?

Procedure:

Verify that the interfaces for Service Discovery (SD) proxies follow KIPs for that Global Information Grid (GIG) Key Interface Profiles (KIPs).

Example:

None.

G1643

Statement:

Comply with the **Federated Search # Registration Web Service** (RWS) **Global Information Grid** (GIG) **Key Interface Profiles** (KIPs) in Node implemented Federated Search # Registration Web Service (RWS).

Rationale:

When a **Federated Search # Registration Web Service** (RWS) is implemented locally, use the **Global Information Grid** (GIG) KIPs developed by **DISA** as the authoritative definition of the interfaces. This allows a **Component** that is hosted by one Node to be hosted on another node with a minimal impact.

Referenced By:

[Content Discovery Services](#)

Evaluation Criteria:

1) **Test:** [G1643.1]

Does a **Federated Search # Registration Web Service** (RWS) used locally within the Node implement the applicable **Global Information Grid** (GIG) **Key Interface Profile** (KIP)?

Procedure:

Verify that the interfaces for Federated Search # Registration Web Service (RWS) implement Global Information Grid (GIG) Key Interface Profiles (KIPs) for that Federated Search # Registration Web Service (RWS).

Example:

None.

G1644

Statement:

Comply with the **Federated Search # Search Web Service** (SWS) **Global Information Grid** (GIG) **Key Interface Profiles** (KIPs) in Node implemented Federated Search # Search Web Service (SWS).

Rationale:

When a **Federated Search # Search Web Service** (SWS) is implemented locally, use the **Global Information Grid** (GIG) **Key Interface Profiles** (KIPs) developed by **DISA** as the authoritative definition of the interfaces. This allows a **Component** that is hosted by one Node to be hosted on another node with a minimal impact.

Referenced By:

Interoperability
Content Discovery Services

Evaluation Criteria:

1) Test: [G1644.1]

Does **Federated Search # Search Web Service** (SWS) used locally within the Node implement the applicable **Global Information Grid** (GIG) **Key Interface Profile** (KIP)?

Procedure:

Verify that the interfaces for Federated Search # Search Web Service (SWS) implement Global Information Grid (GIG) Key Interface Profiles (KIPs) for that Federated Search # Search Web Service (SWS).

Example:

None.

G1645

Statement:

Implement a local **Content Discovery Service** (CDS).

Rationale:

The node should implement the **Content Discovery Service** (CDS) as part of the node infrastructure to be shared among the **Components** hosted at the Node. A CDS will allow other Nodes and Components to find content within the node. The systems within the Node normally provide the content.

Note: *If a Node is frequently disconnected, has intermittent connectivity, or is otherwise isolated, then hosting a local CDS might not be a practical solution for external content discovery and more effective means for internal discovery may be applicable.*

Referenced By:

[Interoperability](#)
[Content Discovery Services](#)

Evaluation Criteria:

1) **Test:** [G1645.1]

Does the Node implement the **Content Discovery Service** (CDS) **Global Information Grid** (GIG) **Key Interface Profile** (KIP)?

Procedure:

Look for an implementation at the Node of the Content Discovery Service (CDS) Global Information Grid (GIG) Key Interface Profiles (KIPs).

Example:

None.

G1646

Statement:

Comply with the directory services **Global Information Grid (GIG) Key Interface Profiles (KIPs)** in Node **Federated Search Services proxies**.

Rationale:

A Node may expose or control access to **Global Information Grid (GIG) Federated Search Services** by using **proxies**. This allows a **Component** that is hosted by one Node to be hosted on another node with a minimal impact.

Referenced By:

Interoperability
Content Discovery Services

Evaluation Criteria:

1) Test: [G1646.1]

Do all **Federated Search Services proxies** locally defined within the Node expose Federated Search Services using the applicable **Global Information Grid KIP**?

Procedure:

Verify that the interfaces for Federated Search Services proxies follow KIPs for that Global Information Grid (GIG) Key Interface Profiles (KIPs).

Example:

None.

G1647

Statement:

Provide access to the **Federated Search** Services.

Rationale:

Content Discovery Service can search across a set of Content Discovery Services and yield an integrated result. The current approach to providing this service is to harness an existing capability termed **Federated Search** developed under the **Horizontal Fusion** (HF) program. The capability utilizes the **DoD Discovery Metadata Specification** (DDMS).

Referenced By:

Content Discovery Services
Design Tenet: Provide Data Management

Evaluation Criteria:

1) Test: [G1647.1]

Does the Node provide access to the **Federated Search** Service **Global Information Grid** (GIG) **Key Interface Profile** (KIP)?

Procedure:

Look for a proxy or an implementation that provides access to the **Federated Search**

Example:

None.

G1652

Statement:

Use DoD **PKI X.509 certificates** for **servers**.

Rationale:

Using a DoD PKI X.509 **server certificate** identifies the server as being trusted by the DoD and guarantees that the server's identity is legitimate.

Referenced By:

[Identity Management](#)
[Design Tenet: Identity Management, Authentication, and Privileges](#)

Evaluation Criteria:

1) **Test:** [G1652.1]

Is the server certificate a valid DoD PKI X.509 certificate that is non-expired?

Procedure:

Open the server certificate and check that it is trusted by a trusted DoD root certificate.

Example:

G1662

Statement:

Follow the guidance provided in the **Security Technical Implementation Guide** (STIG) for **Domain Name System** (DNS) implementations.

Rationale:

As a fundamental common service on **IP**-based networks, **DNS** is often a focal point for network attackers. Following the **STIG** ensures alignment with DoD identified security practices and configurations. The STIG addresses implementation options such as the choice of basic DNS server types (primary, secondary, caching-only), use of a split-DNS design, location of servers in the network and relationship to other network components, secure administration, security of zone transfers, and initial configuration.

Referenced By:

[Domain Name System \(DNS\)](#)
[Other Design Tenets](#)

Evaluation Criteria:

1) **Test:** [G1662.1]

Do the Node's **DNS** services follow the **STIG** for DNS implementations?

Procedure:

Compare Node DNS services configuration with those recommended by the STIG.

Example:

None.

G1667

Statement:

Implement **Virtual Private Networks** (VPNs) in accordance with the guidance provided in the Network **Security Technical Implementation Guide** (STIG).

Rationale:

Virtual Private Networks provide a means for Node access to users outside the security enclave. To Network **STIG** provides recommendations on how to configure VPNs for secure access.

Referenced By:

[Virtual Private Networks \(VPN\)](#)
[Other Design Tenets](#)

Evaluation Criteria:

1) **Test:** [G1667.1]

Does the configuration of the Node's **VPN** servers follow the recommendations of the Network **STIG**?

Procedure:

Check VPN server configuration against recommended configurations in the Network STIG.

Example:

None.

BP1400

Statement:

Programs will use authoritative **metadata** established by the Joint Mission Threads (JMTs) when available.

Rationale:

Referenced By:

[Design Tenet: Joint Net-Centric Capabilities
Data Modeling](#)

BP1594

Statement:

Examine the use of **Transmission Control Protocol** (TCP) extensions and other transport protocols that have been designed to mitigate risk for high bandwidth, high latency satellite communications.

Rationale:

TCP performance over satellite links is generally poor due to delays and blockages inherent to satellite links. TCP extensions (e.g., [IETF RFC 1323](#)) and other transport protocols that have been developed to mitigate this risk should be considered for high bandwidth, high latency satellite communications.

Referenced By:

[Mobile Nodes](#)
[Design Tenet: Transport Goal](#)

Evaluation Criteria:

1) Test: [BP1594.1]

If the system is involved in high bandwidth, high latency satellite communications, does the Node design address TCP performance?

Procedure:

Determine if parts of the system involve high bandwidth, high latency satellite communications and if so, look for a TCP extension.

Example:

None.

BP1597

Statement:

Consider operational performance constraints in the design of the Node's **Domain Name System** (DNS).

Rationale:

Operational performance constraints such as narrow band width or intermittent service can have a large impact in how the **Domain Name System** (DNS) **server** is configured and consequently on the DNS chosen to support the Node.

Referenced By:

[Domain Name System \(DNS\)](#)

Evaluation Criteria:

1) **Test:** [BP1597.1]

Have the operational performance constraints been delineated and used to justify the **Domain Name System** (DNS) used by the Node?

Procedure:

Review the acquisition documents looking for justifications for the selection of the Domain Name System (DNS).

Example:

None.

BP1614

Statement:

Prepare a **Node** for the possibility of becoming a new **Component** service within another Node.

Rationale:

While the complexities of nested Nodes are currently not addressed within NESI Part 4, nested Nodes are a possibility; thus, Nodes should be prepared to interact in such an environment. Following the guidance for Nodes in Part 4 should be sufficient to prepare the Node for such interactions by encouraging the proper definition of key interfaces and capabilities and creating a distinction between Nodal infrastructure and Component capabilities. These distinctions would allow a Node, for example, to supplant it's own infrastructure with those of it's new parent Node (either directly or via proxies).

Note: *The purpose of this practice is not necessarily to encourage nested Nodes, but to ensure that Nodes apply appropriate open **modular designs** both externally and internally to ensure greater interoperability in a variety of environments.*

Referenced By:

[Web Client Platform](#)
[Design Tenet: Cross-Security-Domains Exchange](#)
[Cross-Domain Interoperation](#)

Evaluation Criteria:

1) **Test:** [BP1614.1]

Does the Node use standardized interfaces to obtain the services of routine activities?

Procedure:

Look for alignment and adherence to guidance of NESI Part 4 and open systems approaches.

Example:

None.

BP1615

Statement:

Select **Web browsers** that support a wide breadth of current browser extension technologies.

Rationale:

Web browsers are a key application for allowing users to capitalize on the DoD vision of net-centric information sharing and access to distributed services. In order to ensure maximum interoperability with available services that may not be known a priori, browsers should support current standards and capabilities such as **JavaScript**, **Java applets**, and **plug-ins**.

Referenced By:

[Browser](#)

Evaluation Criteria:

1) **Test:** [BP1615.1]

Does the **Web browser** support commonly accepted browser technologies such as **plug-ins**, **APIs** and scripting languages?

Procedure:

Review the list of tested Web browsers and make sure they support plug-ins, APIs and scripting languages.

Example:

None.

BP1648

Statement:

Host the **Registration Web Service** (RWS) registration **portlet** in the Node.

Rationale:

The process of registering a Node's **Component** service with the **Registration Web Service** (RWS) can be quite complicated. By providing access to the registration **portlet** the chances of obtaining a registration and of having valid data in the registration are greatly increased.

Referenced By:

[Content Discovery Services](#)

Evaluation Criteria:

1) **Test:** [BP1648.1]

Is the **Registration Web Service** (RWS) registration **portlet** hosted on the local Node?

Procedure:

Look for the Registration Web Service (RWS) registration portlet implementation.

Example:

None.

BP1649

Statement:

Specifically include provisions for incremental implementation of the **CES** services.

Rationale:

The states of the individual services that comprise the **CES** are at different level of maturity. Consequently, an incremental approach allows Node development to continue in parallel with the CES functionality.

Referenced By:

[CES Parallel Development](#)

Evaluation Criteria:

1) **Test:** [BP1649.1]

Is there an incremental development approach?

Procedure:

Review the Node's schedule for incremental development.

Example:

None.

BP1650

Statement:

Specifically include provisions for incremental implementation of the hosting Node's **CES** services for Node **Components**.

Rationale:

The states of the individual services that comprise the **CES** are at different levels of maturity. Consequently, an incremental approach allows **Component** development to continue in parallel with the Node and CES functionality.

Referenced By:

[CES Parallel Development](#)

Evaluation Criteria:

1) **Test:** [BP1650.1]

Is there an incremental development approach?

Procedure:

Review the schedule for Components for incremental development.

Example:

None.

BP1651

Statement:

Do not implement **server** side **CES** functionality for **Components**.

Rationale:

The burden of aligning to standard CES functionality and providing the functionality uniformly rests on the Node infrastructure, rather than the **Components** within the Node. This isolates the Components from the **CES** complexity and enhances portability and interoperability of the Components.

Referenced By:

[Design Tenet: Network Connectivity
CES and Intermittent Availability](#)

Evaluation Criteria:

1) **Test:** [BP1651.1]

Do any **Component** systems, applications or services implement any of the server side **CES** Global Information Grid (**GIG**) **Key Interface Profiles** (KIPs)?

Procedure:

Review the Component systems, applications or services code for implementations of the server side CES Global Information Grid (GIG) Key Interface Profiles (KIPs).

Example:

None.

BP1653

Statement:

Do not build dedicated Node guard products.

Rationale:

Current national policy dictates that a high-assurance guard or similar technology must be used whenever connecting networked security domains (i.e., **SECRET US** to **SECRET REL** or **SIPRNET** to **NIPRNET**). Every single instantiation of every single guard needs to be approved by the appropriate authority. There are no type accreditations. Adding a new guard technique will likely incur additional scrutiny of the program as well as significant technical and schedule risks. The preferred approach is to use an already approved guard to mitigate risk.

Referenced By:

[Trusted Guards](#)

BP1654

Statement:

Do not build dedicated **Component** guard products.

Rationale:

Current national policy dictates that a high-assurance guard or similar technology must be used whenever connecting networked security domains (i.e., **SECRET US** to **SECRET REL** or **SIPRNET** TO **NIPRNET**). Every single instantiation of every single guard needs to be approved by the appropriate authority. There are no type accreditations. Adding a new guard technique will likely incur additional scrutiny of the program as well as significant and technical and schedule risks. The preferred approach is to use an already approved guard to mitigate risk.

Referenced By:

[Trusted Guards](#)

BP1661

Statement:

Engage with the **Net-Centric Enterprise Services** (NCES) program office to explore approaches for mobile use of the **Core Enterprise Services** (CES) services in mobile Nodes that rely on **Transmission Control Protocol/Internet Protocol** (TCP/IP) for inter-node communication.

Rationale:

Referenced By:

[CES Definitions and Status](#)
[Design Tenet: Joint Net-Centric Capabilities](#)

BP1663

Statement:

Design a **Domain Name System** (DNS) in coordination with the appropriate governing Internet Protocol Version 6 (IPv6) Transformation Office.

Rationale:

Referenced By:

Design Tenet: IPv6
Domain Name System (DNS)

BP1668

Statement:

Acquire and configure approved guard products with the help of the Government program offices that acquire such guards.

Rationale:

Leveraging the certification documentation, expertise and existing relationships with the **National Security Agency** (NSA) and other pertinent authorities will streamline acquisition of approved guards.

Referenced By:

[Trusted Guards](#)

BP1669

Statement:

Select **XML**-capable **trusted guards**.

Rationale:

As **XML** is a fundamental transfer format for data in interoperable net-centric environments, **trusted guards** should be capable of transferring XML data to facilitate cross-domain interoperability.

Referenced By:

[Design Tenet: Cross-Security-Domains Exchange Trusted Guards](#)

BP1670

Statement:

Monitor Black Core implementation issues and prepare a plan for local implementation in coordination with system programs fielded within the Node.

Rationale:

Referenced By:

Design Tenet: Concurrent Transport of Information Flows
Black Core

BP1671

Statement:

Consider Black Core transition whenever there is a significant Node network design or configuration decision to make in an effort to avoid costly downstream changes caused by Black Core transition.

Rationale:

Referenced By:

[Black Core](#)
[Design Tenet: Concurrent Transport of Information Flows](#)

BP1672

Statement:

Be prepared to integrate fully with the **Information Assurance** (IA) infrastructure.

Rationale:

Referenced By:

[Design Tenet: Net-Centric IA Posture and Continuity of Operations
Web Client Platform](#)

BP1673

Statement:

Be prepared to integrate fully with the **Enterprise Management Services** (EMS) infrastructure.

Rationale:

Referenced By:

[Web Client Platform](#)

BP1674

Statement:

Configure the **browser** in accordance with the Web Server Security Technical Implementation Guide (**STIG**), Desktop Applications STIG, and Windows 2003/XP/2000 Addendum STIG.

Rationale:

Referenced By:

[Browser](#)

BP1675

Statement:

In the Node's Web infrastructure, support the technologies and standards used by the **CES** services under development as well as any technologies and standards used for **Community of Interest** (COI) services.

Rationale:

Referenced By:

[CES Definitions and Status](#)
[Web Infrastructure](#)

BP1677

Statement:

Consider using Web **proxy** servers and load balancers.

Rationale:

Referenced By:

[Web Infrastructure](#)

BP1679

Statement:

Implement a Node that uses **Active Directory** (AD) in accordance with the recommendations of the DoD Active Directory Interoperability Working Group (DADIWG).

Rationale:

The purpose of DoD Active Directory Interoperability Working Group (DADIWG) specification is to define a DoD naming convention for users with the objective of promoting more efficient data synchronization to support email communications for the Joint environment and to prepare **Active Directory** to support more sophisticated DoD-wide directory and discovery services. This specification develops consistent naming conventions # naming formats, content, and supporting data values, for a baseline set of attributes for Active Directory User Objects.

Referenced By:

[Domain Directories](#)

BP1680

Statement:

Instrument **Component** services that a Node exposes to the **Global Information Grid** (GIG) to collect performance metrics.

Rationale:

In a dynamic environment, where services and information exchange partners may be dynamic, metrics can be a key factor in the selection of services. Performance metrics that are advertised externally and frequently updated allow potential service users the ability to select an implementation that meets their performance requirements, such as a measurement of reliability.

Standards for metrics are expected to be defined in the Net-Centric Implementation Directives (NCID) S500 document that is not yet available. Some draft metrics that may be appropriate for web services are given in the following table:

<i>SLA Metric</i>	<i>Metric Description</i>
Availability	How often is the service available for consumption?
Accessibility	How capable is the service of serving a client request now?
Performance	How long does it take for the service to respond?
Compliance	How fully does the service comply with stated standards?
Security	How safe and secure is it to interact with this service?
Energy Efficiency	How energy-efficient is this service for mobile applications?
Reliability	How often does the service fail to maintain its overall service quality?

Referenced By:

[Instrumentation for Metrics](#)

BP1681

Statement:

Make **Component** services metrics visible and accessible as part of the service registration and updated periodically.

Rationale:

Metrics are normally also needed to ensure performance is provided according to more traditional **Service Level Agreements** (SLAs) and for operations management.

Referenced By:

[Instrumentation for Metrics](#)
[Design Tenet: Joint Net-Centric Capabilities](#)

BP1683

Statement:

Coordinate the Node schedule with the **Net-Centric Enterprise Services** (NCES) schedule.

Rationale:

An unavoidable consequence of the Node architecture, is that the CES being developed by **Net-Centric Enterprise Services** (NCES) is occurring in parallel with the development of the Nodes themselves. If the Node's schedule is not coordinated with NCES, Node capabilities will be developed that can not be supported within the NCES infrastructure.

Referenced By:

[CES Definitions and Status](#)
[CES Parallel Development](#)

Evaluation Criteria:

1) **Test:** [BP1683.1]

Is there a Node roadmap that maps to the **Net-Centric Enterprise Services** (NCES) schedule?

Procedure:

Look for a document that cross-references the Net-Centric Enterprise Services (NCES) schedule of capabilities to the Node's schedule.

Example:

None.

BP1684

Statement:

Coordinate the Node schedule with the **Component** schedules.

Rationale:

All schedules are subject to slippage or modifications due to changing priorities. If the **Net-Centric Enterprise Services** (NCES) schedule changes or the development of certain Node capabilities is changed, there can be an impact to a Node's **Component's** schedules.

Referenced By:

[CES Definitions and Status](#)
[CES Parallel Development](#)

BP1685

Statement:

For **Key Interface Profile** (KIP) specifications that are not available or insufficiently mature, implement a "best effort" by following the published intent of functionality and monitor or participate in the relevant specification development body.

Rationale:

Referenced By:

[Key Interface Profile \(KIP\)](#)

BP1686

Statement:

Align Node interfaces to **Components** for directory services with the guidance being provided by the Joint Enterprise Directory Services Working Group (JEDIWG) and sub-working groups, including such guidance as naming conventions, federation, and synchronization.

Rationale:

Referenced By:

[Design Tenet: Joint Net-Centric Capabilities Directory Services](#)

BP1687

Statement:

Follow **Active Directory** naming conventions defined in the *Active Directory User Object Attributes Specification* as required by the DoD **CIO** memorandum titled *Microsoft Active Directory (AD) Services*.

Rationale:

Referenced By:

[Directory Services](#)

BP1688

Statement:

For **Services Management**, use an interim solution of instrumentation of services and external monitoring.

Rationale:

This interim solution provides potential service consumers with real world historical performance metrics as well ensures that negotiated **SLAs** are supported.

Referenced By:

[Services Management](#)

BP1689

Statement:

Use the **Service Discovery** (SD) pilot program to practice and exercise the mechanics of service discovery and late binding.

Rationale:

The pilot program provides an opportunity to practice and exercise the mechanics of **Service Discovery** (SD) and late binding.

Referenced By:

[Service Discovery](#)
[Design Tenet: Service-Oriented Architecture \(SOA\)](#)

BP1690

Statement:

Use Node implemented **Service Discovery** (SD) for high availability.

Rationale:

One of the main reasons to develop a local Node **Service Discovery** (SD) Service is to support high availability.

Referenced By:

[Service Discovery](#)

BP1691

Statement:

Use **Node** implemented **Service Discovery (SD)** to meet compartmentalization needs.

Rationale:

For pilot implementations that are not reachable, such as might be the case in a higher classified environment, the Nodes should coordinate among themselves and DISA to provide pilot and full service implementations that are reachable.

Referenced By:

[Design Tenet: Cross-Security-Domains Exchange](#)
[Cross-Domain Interoperation](#)
[Service Discovery](#)

BP1692

Statement:

Determine which Collaboration Service vendor offering to employ in a disadvantaged environment or separate network.

Rationale:

Monitor progress on fielding the NCES Collaboration Service. Performance or administration reasons may dictate hosting a collaboration solution at the Node.

Referenced By:

[Collaboration Services](#)

BP1693

Statement:

Make sure that **collaboration** products used to satisfy urgent requirements are from the **JTIC** list.

Rationale:

See <http://jtc.fhu.disa.mil/washops/jtcd/dcts/status.html> and, for products certified for use on SIPRNET, <http://jtc.fhu.disa.mil/washops/jtcd/dcts/projects.html>), until the **Net-Centric Enterprise Services** (NCES) Collaboration Service is available.

Referenced By:

[Collaboration Services](#)

BP1694

Statement:

Coordinate with other Nodes having the same compartmentalization needs and with **DISA** to host compartmentalization CES.

Rationale:

The **CES** services will be provisioned by **DISA** and operated on the **Non-secure Internet Protocol Router Network** (NIPRNET) and **Secret Internet Protocol Router Network** (SIPRNET) global networks, initially operating from DISA Enterprise Computing Centers (DECCs). In order to have the **CES** to operate within a particular compartmentalization, a proactive role must be taken by the Node.

Referenced By:

[CES Parallel Development](#)

BP1695

Statement:

Designate a **CES** liaison to monitor the availability of services.

Rationale:

The CES liaison is an important role for keeping the Node and **Component** engineering processes synchronized with the **Net-Centric Enterprise Services** (NCEs).

Referenced By:

[CES Parallel Development](#)

BP1696

Statement:

Use the Early Adopter process and service pilots to accelerate implementation of the **CES** services within the Node.

Rationale:

To accelerate the maturation and implementation of the CES, DISA established an Early Adopter process. Early adopters can participate in service pilots, as described in the Pilot Participant's Guide (draft).

Use the Early Adopter process and service pilots to accelerate implementation of the CES services within the Node. The decision to participate in the early adopter process and pilots is influenced by many factors, including acquisition phase, funding, mission, and priorities for individual systems as well as the aggregate Node.

Referenced By:

[CES Parallel Development](#)

BP1697

Statement:

Make the parallel development of **CES** outside the control of the Node a part of the Node's risk management activities.

Rationale:

Since the development of the **CES** is external to the development of the Node, there is an interdependency between the Node and the CES. The Node needs to consider this as an increase in the risk to the Node development. This risk needs to be communicated back to the CES management and development teams.

Referenced By:

[CES Parallel Development](#)

BP1698

Statement:

Plan for the event that **Component** services within a **Node** cannot be invoked across security domains.

Rationale:

Until such approaches are prototyped and explored more fully, Nodes should anticipate that services will not be capable of cross-domain invocation.

Referenced By:

[Cross-Domain Interoperation](#)
[Design Tenet: Cross-Security-Domains Exchange](#)

BP1699

Statement:

Configure **routers** in accordance with the Network **Security Technical Implementation Guide** (STIG).

Rationale:

Referenced By:

[Routers](#)

BP1700

Statement:

Configure **routers** in accordance with Enclave **Security Technical Implementation Guide** (STIG).

Rationale:

Referenced By:

[Routers](#)

BP1701

Statement:

Configure **Components** for **Information Assurance** (IA) in accordance with the Network **Security Technical Implementation Guide** (STIG).

Rationale:

Referenced By:

Design Tenet: Net-Centric IA Posture and Continuity of Operations
Network Information Assurance

BP1702

Statement:

Do not place services and information intended to be broadly accessible to other nodes behind a **Virtual Private Network** (VPN).

Rationale:

Referenced By:

[Virtual Private Networks \(VPN\)](#)

BP1704

Statement:

Consult the applicable **Security Technical Implementation Guidance** (STIG) documents as a fundamental part of design activities, and monitor the STIGs periodically for updates.

Rationale:

Referenced By:

[Node Transport](#)

BP1705

Statement:

Design **DNS** infrastructure in accordance with appropriate governing **IPv6** Transition Office requirements.

Rationale:

Referenced By:

IPv4 to IPv6 Transition
Domain Name System (DNS)
Design Tenet: IPv6

BP1706

Statement:

Design node networks, including the selection of **Components** and configuration, to support **multicasting** even if not currently used.

Rationale:

The use of multicasting is growing within the DoD and multicast capability is being actively engineered into the **Global Information Grid (GIG)**.

Referenced By:

[Multicast](#)

BP1707

Statement:

Configure and locate elements of the Node Web infrastructure in accordance with the Web Server **Security Technical Implementation Guide** (STIG).

Rationale:

Referenced By:

[Web Infrastructure](#)

BP1708

Statement:

Configure and locate elements of the Node Web infrastructure in accordance with the Desktop Applications **Security Technical Implementation Guide** (STIG).

Rationale:

Referenced By:

[Web Infrastructure](#)

BP1709

Statement:

Configure and locate elements of the Node Web infrastructure in accordance with the Network **Security Technical Implementation Guide** (STIG).

Rationale:

Referenced By:

[Web Infrastructure](#)

BP1710

Statement:

Support appropriate and widely accepted standards for Web portals provided by the Node.

Rationale:

Referenced By:

[Web Portal](#)

BP1711

Statement:

Use the **CES** Mediation Service, or a locally hosted copy, when **XML** document translation between **schemas** is a necessity.

Rationale:

Referenced By:

[Mediation Services](#)

BP1712

Statement:

Register developed mappings in the **DoD Metadata Registry**.

Rationale:

Referenced By:

Mediation Services
Design Tenet: Joint Technical Architecture [now DISR]

BP1824

Statement:

Use the `USER_DATA` **Quality of Service** (QoS) to communicate metadata on the `DomainParticipant` that may be used to authenticate the application trying to join the Data **Distribution Service** (DDS) `Domain`.

Rationale:

In many cases the application needs to send additional information that describes the `DomainParticipant` to other participants in the DDS Domain. This information can be used to authenticate the participant or to meet any other application-specific need.

The `USER_DATA` QoS on the `DomainParticipant` allows the application to store un-interpreted bytes that will be propagated via the DDS built-in discovery mechanism and will be accessible to the other `DomainParticipants` on the system.

Referenced By:

[DDS Quality of Service](#)

Evaluation Criteria:

1) **Test:** [BP1824.1]

Is the `USER_DATA` QoS set on the `DomainParticipant`?

Procedure:

Check the creation of the `DomainParticipant` and determine whether the `USER_DATA` QoS is used. Ensure that the application does not use another non-standard way to accomplish the same function.

Example:

None.

BP1826

Statement:

Use the **USER_DATA Quality of Service** (QoS) on the **DataWriters** and **DataReaders** to communicate metadata that may provide application-specific information of the entity writing/reading data in a **Data Distribution Service** (DDS) **Domain**.

Rationale:

In many cases the application needs to send additional information that describes the **DataWriter** or the **DataReader** to other entities in the DDS Domain. This information can be used to authenticate the **DataWriter/Reader** or to meet any other application-specific need.

The **USER_DATA** QoS on the **DataWriter** and the **DataReader** allows the application to store un-interpreted bytes that will be propagated via DDS's built-in discovery mechanism and will be accessible to the other **DataWriters** and **DataReaders** on the system.

Referenced By:

[DDS Quality of Service](#)

Evaluation Criteria:

1) **Test:** [BP1826.1]

Is the **USER_DATA** QoS set on the **DataWriter** and **DataReader**?

Procedure:

Check the creation of the **DataWriter** and **DataReader** and determine whether the **USER_DATA** QoS is used. Ensure that the application does not use another non-standard way to accomplish the same function.

Example:

None.

BP1863

Statement:

Make shareable data assets visible, even if they are not accessible.

Rationale:

Making data visible using a consistent, standardized metadata specification within a Net-Centric Environment (NCE) facilitates a federated cross-organizational discovery capability [R1172]. A common specification for the description of information allows for a comprehensive capability that can locate all information across the NCE regardless of format, type, location, or classification, dependent on user authorization. The **DoD Metadata Specification (DDMS)** was developed to support Enterprise-wide data discovery by providing a common set of descriptive metadata elements. Discovery metadata must conform to the DDMS in accordance with DoD Directive (DoDD) 8320.2 [R1217]. Information owners tag information with DDMS-compliant metadata to ensure discoverability of information in the NCE.

The extensible nature of the DDMS supports domain-specific or **COI** discovery metadata requirements and extends the element categories identified in the DDMS Core Layer used to describe information. Use of the DDMS does not preclude use of other metadata processes or standards. For example, record-level database tagging and in-line document tagging are common practices to support various department objectives. These tagging initiatives should be enhanced to include the DDMS for enterprise discovery.

Referenced By:

[Design Tenet: IPv6](#)
[Net-Centric Data Strategy \(NCDS\)](#)
[Design Tenet: Make Data Visible](#)
[Design Tenet: Open Architecture](#)
[Design Tenet: Service-Oriented Architecture \(SOA\)](#)

Evaluation Criteria:

1) Test: [BP1863.1]

Does the system provide discovery metadata in accordance with the DoD Discovery Metadata Standard (DDMS) for all data posted to shared spaces?

Procedure:

Examine the DoD Metadata Registry for program/system.

Example:

Discoverable information has associated DDMS metadata that can be found in the DDMS).

BP1865

Statement:

Provide sufficient program, project, or initiative **metadata** descriptions and automated support to enable **mediation** and translation of the data between **interfaces**.

Rationale:

Information exchanges should support known and unanticipated users. The program or project should initiate sufficient metadata descriptions and provide automated support to enable mediation and translation of data between interfaces. All of the data that can and should be shared externally beyond the programmatic bounds of your program should be defined well enough in metadata descriptions and translation of the data between interfaces should be automated.

Referenced By:

[Content Discovery Services](#)
[Net-Centric Data Strategy \(NCDS\)](#)
[Design Tenet: Provide Data Management](#)
[Design Tenet: Make Data Visible](#)
[Net-Centric Information Engineering](#)
[Metadata](#)
[Coordination of Node and Enterprise Services](#)
[Design Tenet: Make Data Interoperable](#)

Evaluation Criteria:

1) Test: [BP1865.1]

Evaluation of interfaces and applicable mediation/translations to access that the program, project, or initiative has sufficient metadata descriptions and automated support to enable mediation and translation of the data between interfaces. Data is XML wrapped for exchange and configured to support standard transactions with headers, trailers and bodies.

Procedure:

Evaluate the degree to which data is XML wrapped for exchange and configured to support standard transactions with headers, trailers and bodies.

Evaluation of the DoD Metadata Registry entries to assess sufficient metadata descriptions and automated support the enables mediation and translation of the data between interfaces.

Example:

XML wrapped data are intend for exchange, that is configured in terms of standard transactions with headers, trailers and bodies.

BP1866

Statement:

Coordinate with end users to develop interoperable materiel in support of high-value mission capability.

Rationale:

System providers acquire the materiel portion of mission capabilities that include all aspects of DOTMLP-F. An assessment by the community regarding the value of information or services provides useful direction in support of managing a mission area's portfolio of services. User feedback mechanisms provide a means of capturing and reporting user satisfaction and give portfolio managers decision-making information to steer investments, developments, and improvements. As service consumers gain access to information more quickly in the operational environment, command structures will inevitably change the manner in which IT investments are made. Service and information providers in a mission area should work together to define the processes for using the user feedback for service and information improvements because these processes are specific to a portfolio of capabilities in the Enterprise.

Referenced By:

[Design Tenet: Make Data Interoperable](#)
[Net-Centric Information Engineering](#)
[Design Tenet: Joint Net-Centric Capabilities](#)

Evaluation Criteria:

1) Test: [BP1866.1]

Processes exist that allow a consumer to

1. request changes in the format (syntax or semantic) of the visible data asset;
2. report a problem with a data asset;
3. request additional data from the data provider

Procedure:

Evaluation of the process a consumer would follow to

1. request changes in the format (syntax or semantic) of the visible data asset;
2. report a problem with a data asset;
3. request additional data from the data provider.

Example:

An end-to-end output management strategy, across multiple business sites and/or the enterprise.

A distributed and extensible database which make information accessible to authorized users across the enterprise.

BP1867

Statement:

Use metrics to track responsiveness to user information sharing needs.

Rationale:

Information sharing metrics are defined to measure and track implementation of the net-centric approaches. Measurement techniques should be developed to ensure that metrics are captured in a useful and consistent manner. Metrics should be tagged with **DDMS**-compliant metadata and provided to the NCE to promote awareness of data management successes and areas requiring improvement.

Referenced By:

[Design Tenet: Be Responsive to User Needs
Instrumentation for Metrics](#)

Evaluation Criteria:

1) **Test:** [BP1867.1]

Does the program, project or initiative have metrics for determining responsiveness to user needs?

Procedure:

Evaluate the metrics being used to determine responsiveness to user data needs. If YES, describe; If NO, explain and identify a time frame for when the program, project, or initiative will have metrics for determining responsiveness to user needs; or specify NOT APPLICABLE and explain.

Example:

Examples of data metrics include percentage of Web-enabled components, progress toward service-enabling identified key functional components, and percentage of tagged community data.

Glossary

.NET		<p>To address the confusing maze of computer languages, libraries, tools, and toolkits that were necessary for creating multi-tier applications, Microsoft developed the .NET Framework and integrated it into Microsoft Windows as a component. It supports building and running multi-tier and service-oriented architectures, including Web services and client and server applications. It simplifies the process of designing, developing, and testing software, allowing individual developers to focus on core, application-specific code.</p>
Access Control		<p>Limiting access to information system resources only to authorized users, programs, processes, or other systems. (Source: National Information Assurance (IA) Glossary, CNSSI 4009, revised June 2006)</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Note: See also the following:</p> <ul style="list-style-type: none"> • Access Control List (ACL) [GL1889] • Discretionary Access Control (DAC) [GL1197] • Role-Based Access Control (RBAC) [GL1643] </div>
Access Control List	ACL	<p>In computer security, ACL is a concept used to enforce privilege separation. It is a means of determining the appropriate access rights to a given object depending on certain aspects of the process that is making the request, principally the process's user identity.</p> <p>In networking, ACL refers to a list of ports and services that are available on a host, each with a list of hosts and/or networks permitted to use the service. Both individual servers as well as routers can have access lists. Access lists are used to control both inbound and outbound traffic, and in this context they are similar to firewalls. (Source: http://en.wikipedia.org/wiki/Access_control_list)</p>
Active Directory	AD	<p>An implementation of Lightweight Directory Access Protocol (LDAP) directory services by Microsoft for use in Windows environments; allows administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization. An Active Directory stores information and settings relating to an organization in a central, organized, accessible database. Active Directory networks can vary from a small installation with a few hundred objects, to a large installation with millions of objects. (Source: http://en.wikipedia.org/wiki/Active_Directory)</p>

Part 4: Node Guidance

All Views	AV	<p>The DoDAF All-Views (AV) products provide information pertinent to the entire architecture but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture. The scope includes the subject area and timeframe for the architecture. The setting in which the architecture exists comprises the interrelated conditions that compose the context for the architecture. These conditions include doctrine; tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations; scenarios; and environmental conditions. (Source: <i>DoDAF v1.5 Volume 1: Definintions and Guidelines</i>, 23 April 2007)</p>
American Standard Code for Information Interchange	ASCII	<p>ASCII is a character set and a character encoding based on the Roman alphabet as used in modern English (see English alphabet). ASCII codes represent text in computers, in other communications equipment, and in control devices that work with text. Most often, nowadays, character encoding has an ASCII-like base.</p> <p>ASCII defines the following printable characters, presented here in numerical order of their ASCII value:</p> <pre data-bbox="667 835 1427 940">!"#\$%&'()*+,-./0123456789:;? @ABCDEFGHIJKLMNPQRSTUVWXYZ[\]^_ `abcdefghijklmnopqrstuvwxyz{ }~(</pre> <p>(Source: http://en.wikipedia.org/wiki/ASCII)</p>
Applet		<p>A J2EE component that typically executes in a Web browser. Applets can also execute in a variety of other applications or devices that support the applet programming model. (Source: <i>J2EE 1.4 Glossary</i>, http://java.sun.com/j2ee/1.4/docs/glossary.html)</p>
Application		<p>Provides the resources necessary to provision, operate and maintain Net-Centric Enterprise Services (NCES) capabilities.</p>
Application Programming Interface	API	<p>A special type of interface that specifies the calling conventions with which one component may access the resources and services provided by another component. APIs are defined by sets of procedures or function-invocation specifications. An API is a special case of an interface.</p>
Assistant Secretary of Defense for Networks and Information Integration	ASD (NII)	<p>(Source: http://www.dod.mil/nii/)</p>

Part 4: Node Guidance

Attribute		A distinct characteristic of an object. Real-world object attributes are often specified in terms of their physical traits, such as size, shape, weight, and color. Cyberspace object attributes might describe size, type of encoding, and network address. (Source: http://www.oasis-open.org/committees/download.php/3343/oasis-200304-wsrp-specification-1.0.pdf)
Authentication		The process that verifies the identity of a user, device, or other entity in a computer system, usually as a prerequisite to allowing access to resources in a system. The Java servlet specification requires three types of authentication (basic, form-based, and mutual) and supports digest authentication. (Source: <i>J2EE 1.4 Glossary</i> , http://java.sun.com/j2ee/1.4/docs/glossary.html)
Authorization		The process by which access to a method or resource is determined. Authorization depends on the determination of whether the principal associated with a request through authentication is in a given security role. A security role is a logical grouping of users defined by the person who assembles the application. A deployer maps security roles to security identities. Security identities may be principals or groups in the operational environment. (Source: <i>J2EE 1.4 Glossary</i> , http://java.sun.com/j2ee/1.4/docs/glossary.html)
Browser		Short for Web browser , a software application used to locate and display Web pages. (Source: http://www.webopedia.com/TERM/b/browser.html)
Capability Development Document	CDD	Provides operational performance attributes, including supportability, for the acquisition community to design the proposed system. Includes key performance parameters (KPP) and other parameters that guide the development, demonstration, and testing of the current increment. Outlines the overall strategy for developing full capability. (Source: http://www.dau.mil/pubs/glossary/12th_Glossary_2005.pdf)
Capability Production Document	CPD	Addresses the production attributes and quantities specific to a single increment of an acquisition program. Supersedes threshold and objective performance values of the CDD. (Source: http://www.dau.mil/pubs/glossary/12th_Glossary_2005.pdf)
Certificate	CERT	A certificate which uses a digital signature to bind together a public key with an identity information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. (Source: http://en.wikipedia.org/wiki/Certificate_%28cryptography%29)
Certificate Revocation List	CRL	A list of certificates (more accurately, their serial numbers) which have been revoked, are no longer valid, and should not be relied upon by any system user. (Source: http://en.wikipedia.org/wiki/Certificate_Revocation_List)
Chief Information Officer	CIO	Job title for a manager responsible for Information Technology (IT) within an organization; often reports to the chief executive officer or chief financial officer. For information

Part 4: Node Guidance

		on the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII)/DoD CIO see DoDD 5144.1 of 2 May 2005. (Source: http://en.wikipedia.org/wiki/Chief_Information_Officer)
Cipher Text	CT	Data that has been encrypted . Cipher text is unreadable until it has been converted into Plain Text (PT) (decrypted) with a key. (Source: http://www.webopedia.com/TERM/C/cipher_text.html)
Client		A system entity that accesses a Web service. (Source: http://www.oasis-open.org/committees/download.php/3343/oasis-200304-wsrp-specification-1.0.pdf)
COI Service		See Community of Interest Service .
Collaboration		Portal members can communicate synchronously through chat or messaging, or asynchronously through threaded discussion, blogs, and email digests (forums).
Collaboration Management Office	CMO	DISA organization responsible for fielding, sustaining and managing the life cycle of the Defense Collaboration Tool Suite (DCTS).
Command, Control, Communications, Computers, and Intelligence, Surveillance, and Reconnaissance	C4ISR	
Commercial Off-The-Shelf	COTS	A term for systems that are manufactured commercially, and may be tailored for specific uses. (Source: http://en.wikipedia.org/wiki/Commercial_off-the-shelf)
Common Access Card	CAC	A DoD-wide smart card used as the identification card for active duty Uniformed Services personnel (to include the Selected Reserve), DoD civilian employees, eligible contractor personnel, and eligible foreign nationals; the primary platform for the Public Key Infrastructure (PKI) authentication token used to access DoD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment; and the principal card enabling physical access to buildings, facilities, installations, and controlled spaces as described in DoD Directive 8190.3, "Smart Card Technology," 31 August 2002. (Source: DoD Instruction 8520.2 , 1 April 2004, [R1206] Enclosure (2) Definitions, page 13)
Common Gateway Interface Script	CGI Script	CGI is a standard for interfacing external applications with information servers, such as HTTP or Web servers. A plain HTML document that the Web daemon retrieves is static, which means it exists in a constant state: a text file that doesn't change. A CGI program, on the other hand, is executed in real time, so it can output dynamic information.
Common Object Request Broker Architecture	CORBA	CORBA "wraps" code written in another language into a bundle containing additional information on the capabilities of the code inside, and explaining how to call it. The resulting

Part 4: Node Guidance

		wrapped objects can then be called from other programs (or CORBA objects) over the network. The CORBA specification defines APIs, communication protocol, and object/service information models to enable heterogeneous applications written in various languages running on various platforms to interoperate. (Source: http://en.wikipedia.org/wiki/CORBA)
Community of Interest	COI	A COI is a collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information it exchanges. (Source: DoDD 8320.02 , 2 December 2004, <i>Data Sharing in a Net-Centric Department of Defense</i>)
Community of Interest Service		A service that may be offered to the enterprise, but is owned and operated by a Community of Interest to provide or support a well-defined set of mission functions and associated information.
Complex Data		Complex data can be represented in a complex data structure or can be mapped into a relational or flat structure with additional metadata provided to represent the complex relationships.
Component		One of the parts that make up a system. A component may be hardware or software and may be subdivided into other components. Note the terms module , component , and unit are often used interchangeably or defined to be sub-elements of one another in different ways depending on the context. The relationship of these terms is not yet standardized. (Source: IEEE Std 610.12-1990) <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p>Note: See system component and software component.</p> </div>
Computer Network Defense	CND	Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. (Source: http://www.dtic.mil/doctrine/jel/doddict/data/c/01182.html)
Computer Network Defense Service Provider	CNDSP	Those organizations responsible for delivering protection, detection and response services to its users. CNDSP providers must provide for the coordination service support of a CNDSP/CA. CNDSP is commonly provided by a Computer Emergency or Incident Response Team (CERT/CIRT) and may be associated with a Network Operations (NetOps) and Security Center (NOSC). (Source: DoD Directive O-8530.1, Computer Network Defense (CND), 8 January 2001, Enclosure 2 Definitions, p. 12)
Content Discovery Service	CDS	Net-Centric Enterprise Services (NCES) service that provided a Federated Search capability.
Core Enterprise Services	CES	Ubiquitous, common solution services that provide capabilities essential to the operation of the enterprise. Generic information services that apply to any COI , provide the basic ability to search the enterprise for desired

Part 4: Node Guidance

		information, and then establish a connection to the desired service. (Source: http://www.defenselink.mil/nii/org/cio/doc/GIG_ES_Core_Enterprise_Services_Strategy_V1-1a.pdf)
Data-Centric		An approach for the design and implementation of systems, applications, services or software that emphasis the data rather than the operations. It implies that the data is physically separated from the code and consequently can be maintained independently (loose coupling between code and data).
Data Distribution Service for Real-Time Systems	DDS	DDS is a recently-adopted OMG standard that is the first open international middleware standard directly addressing publish-subscribe communications for real-time and embedded systems. DDS introduces a virtual Global Data Space where applications can share information by simply reading and writing data-objects addressed by means of an application-defined name (Topic) and a key. DDS features fine and extensive control of QoS parameters, including reliability, bandwidth, delivery deadlines, and resource limits. DDS also supports the construction of local object models on top of the Global Data Space. (Source: OMG Data Distribution Portal, http://portals.omg.org/dds)

Part 4: Node Guidance

Data Element		<p>A data element is an atomic unit of data that has the following:</p> <ul style="list-style-type: none"> • an identification such as a data element name • a clear data element definition • one or more representation terms • optional enumerated values
Data Element Gallery		<p>The Data Element Gallery is an important component of the Metadata Registry and Clearinghouse. The Data Element Gallery provides its users with access to data elements that are commonly used by the Department of Defense such as country codes and U.S. state codes. Users may search the registry, compare data elements, and download an Access database containing the available elements. See the DoD Metadata Registry, http://metadata.dod.mil.</p>
DDS DataReader		<p>The DDS DataReader acts as a typed (i.e., dedicated to only one application data type) accessor to a subscriber. The DataReader class allows the application to declare the data it wishes to receive (i.e., make a subscription) and access the data received by the attached Subscriber.</p>
DDS DataWriter		<p>A DDS DataWriter acts as a typed (i.e., dedicated to only one application data type) accessor to a publisher. The DataWriter class allows the application to set the value of the data to be published under a given Topic.</p>
DDS DomainParticipant		<p>A DDS domain participant represents the local membership of the computer process in a domain. A domain is a distributed concept that links all the computer processes able to communicate with each other. It represents a communication plane; only the publishers and the subscribers attached to the same domain may interact. A computer process can run on the behalf of some user or application.</p>
DDS Global Data Space		<p>Underlying any data-centric publish subscribe system is a data model. In DDS, this model defines the global data space and specifies how Publishers and Subscribers refer to portions of this space. (See DDS Domain)</p>
DDS Publication		<p>A DDS publication is defined by the association of a DataWriter to a publisher. This association expresses the intent of the application to publish the data described by the DataWriter in the context provided by the publisher.</p>
DDS Publisher		<p>A DDS publisher is an object responsible for data distribution. It may publish data of different data types. The DataWriter is the object the application must use to communicate to a publisher the existence and value of data-objects of a given type. When data-object values have been communicated to the publisher through the appropriate DataWriter, it is the publisher's responsibility to perform the distribution (the publisher will do this according to its own QoS, or the QoS attached to the corresponding DataWriter).</p>

Part 4: Node Guidance

DDS Subscriber		A DDS subscriber is an object responsible for receiving published data and making it available (according to the Subscriber's QoS) to the receiving application. It may receive and dispatch data of different specified types. To access the received data, the application must use a typed DataReader attached to the subscriber.
DDS Subscription		A DDS subscription is defined by the association of a DataReader with a subscriber. This association expresses the intent of the application to subscribe the data described by the DataReader in the context provided by the subscriber .
Defense Acquisition University	DAU	The mission of the DAU is to provide practitioner training, career management, and services to enable the DoD Acquisition, Technology & Logistics (AT&L) community to make smart business decisions and deliver timely and affordable capabilities to the warfighter. (Source: http://www.dau.mil/about-dau/docs/mission_vision.ppt)
Defense Collaboration Tool Suite	DCTS	A flexible, integrated set of applications providing interoperable, synchronous, and asynchronous collaboration capability to the Department of Defense Agencies, Combatant Commands, and Military Services. (Source: http://www.disa.mil/main/prodsol/dcts.html)
Defense Enterprise Computing Center	DECC	DISA's five Defense Enterprise Computing Centers (DECCs) and their detachments operate hardware and software encompassing a broad spectrum of computing, storage and communications technologies. (Source: http://www.disa.mil/main/about/csc.html)
Defense Information System Network	DISN	The Defense Information System Network (DISN) has been the Department of Defense's enterprise network for providing data, video and voice services for more than 40 years. (Source: http://www.disa.mil/main/support/dss.html)
Defense Information Systems Agency	DISA	Combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war. (Source: http://www.disa.mil/main/about/missman.html)
Defense IT Standards Registry	DISR	The DoD IT Standards Registry (DISR) is an online repository (http://disronline.disa.mil) for a minimal set of primarily commercial IT standards formerly captured in the Joint Technical Architecture (JTA), Version 6.0. These standards are used as the "building codes" for all systems being procured in the Department of Defense. Use of these building codes facilitates interoperability among systems and integration of new systems into the Global Information Grid (GIG). In addition, the DISR provides the capability to build profiles of standards that programs will use to deliver net-centric capabilities. (Source: http://akss.dau.mil/dag/GuideBook/IG_c7.2.4.2.asp)
Department of Defense	DoD	A civilian Cabinet organization of the United States government. The Department of Defense controls the U.S.

Part 4: Node Guidance

		<p>military and is headquartered at The Pentagon. It is headed by the Secretary of Defense. (Source: http://en.wikipedia.org/wiki/United_States_Department_of_Defense)</p>
Design Pattern		<p>General repeatable solution to a commonly-occurring problem in software design. A design pattern isn't a finished design that can be transformed directly into code; it is a description or template for how to solve a problem that can be used in many different situations. (Source: http://en.wikipedia.org/wiki/Design_pattern_%28computer_science%29)</p>
Directory Service		<p>A directory service organizes computerized content and runs on a directory server computer. It is not to be confused with the directory itself, which is the database that holds the information about objects that are to be managed by the directory service. The directory service is the interface to the directory and provides access to the data that is contained in that directory. It acts as a central authority that can securely authenticate resources and manage identities and relationships between them. (Source: http://en.wikipedia.org/wiki/Directory_service)</p>
Discovery		<p>Search, locate or publish data (content), other capabilities (services), or users across the Global Information Grid (GIG).</p>
Discretionary Access Control	DAC	<p>Defines basic access control policies to objects in a file system. Generally, these are done at the discretion of the object owner: file/directory permissions and user/group ownership. (Source: http://en.wikipedia.org/wiki/Discretionary_access_controlhttp://en.wikipedia.org/wiki/Discretionary_access_control)</p>
Document Type Definition	DTD	<p>An optional part of the XML document prolog, as specified by the XML standard. The DTD specifies constraints on the tags and tag sequences that can be in the document. The DTD has a number of shortcomings, however, and this has led to various schema proposals. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)</p>
DoD Architecture Framework		

Part 4: Node Guidance

DoD Metadata Registry		<p>As part of the overall DoD Net-Centric Data Strategy, the DoD CIO established the DoD Metadata Registry (http://metadata.dod.mil) and a related metadata registration process for the collection, storage and dissemination of structural metadata information resources (schemas, data elements, attributes, document type definitions, style-sheets, data structures, etc.). This Web-based repository is designed to also act as a clearinghouse through which industry and government coordination on metadata technology and related metadata issues can be advanced. As OASD's Executive Agent, DISA maintains and operates the DoD Metadata Registry and Clearinghouse under the direction and oversight of OASD(NII). (Source: DoD Metadata Registry v6.0 Web site, https://metadata.dod.mil/mdr/about.htm)</p>
DoD Net-Centric Data Strategy		<p>This Strategy lays the foundation for realizing the benefits of net-centricity by identifying data goals and approaches for achieving those goals. To realize the vision for net-centric data, two primary objectives must be emphasized: (1) increasing the data that is available to communities or the Enterprise and (2) ensuring that data is usable by both anticipated and unanticipated users and applications. (Source: <i>Department of Defense Net-Centric Data Strategy</i>, DoD CIO, 9 May 2003, http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf)</p>
Domain		<p>A group of related items within a certain area of interest. In DDS, a domain is the basic construct used to bind individual publications and subscriptions together for communication. A distributed application can elect to use single or multiple domains for its data-centric communications. Domains isolate communication, promote scalability and segregate different classifications of data. (See Global Data Space)</p>
Domain Name System	DNS	<p>The Domain Name System stores information about hostnames and domain names in a type of distributed database on networks, such as the Internet. Of the many types of information that can be stored, most importantly it provides a physical location (IP address) for each domain name, and lists the mail exchange servers accepting email for each domain.</p> <p>The DNS provides a vital service on the Internet as it allows the transmission of technical information in a user-friendly way. While computers and network hardware work with IP addresses to perform tasks such as addressing and routing, humans generally find it easier to work with hostnames and domain names (such as www.example.com) in URLs and email addresses. The DNS therefore mediates between the needs and preferences of humans and of software.</p>
Dual Stacking		<p>Incorporating both IPv4 and IPv6 support in routers and computers.</p>
Dynamic Host Configuration Protocol	DHCP	<p>A protocol for assigning dynamic Internet Protocol (IP) addresses to devices on a network; DHCP a device can have</p>

Part 4: Node Guidance

		a different IP address every time it connects to the network. (Source: http://www.webopedia.com/TERM/D/DHCP.html)
Electronic Data Interchange Personnel Identifier	EDI-PI	A unique number assigned to each recipient of a Common Access Card (CAC), which is issued by the United States Department of Defense through the Defense Enrollment Eligibility Reporting System (DEERS). (Source: http://en.wikipedia.org/wiki/Electronic_Data_Interchange_Personal_Identifier)
Encryption		Encryption is the process of obscuring information to make it unreadable without special knowledge. While encryption has been used to protect communications for centuries, only organizations and individuals with an extraordinary need for secrecy have made use of it. In the mid-1970s, strong encryption emerged from the sole preserve of secretive government agencies into the public domain, and is now employed in protecting widely-used systems, such as Internet e-commerce, mobile telephone networks and bank automatic teller machines. (Source: http://en.wikipedia.org/wiki/Encryption)
Enterprise		<p>An organization considered as an entity or system that includes interdependent resources (e.g., people, organizations, and technology) that must coordinate functions and share information in support of a common mission or a set of related missions.</p> <p>In the computer industry, the term is often used to describe any large organization that utilizes computers. An intranet, for example, is a good example of an enterprise computing system. (Source: http://www.webopedia.com/TERM/e/enterprise.html)</p>
Enterprise Management Service	EMS	Enterprise Management Services (EMS) which are often used internal to a node, using a variety of COTS tools, which are fundamental to execution of Service Level Agreements (SLAs).
Enterprise Service		A service that provides capabilities to the enterprise. See also Core Enterprise Service and Community of Interest Service .
Enterprise Service Bus	ESB	A layer of middleware through which a core set of reusable business services are made available.
eXtensible Markup Language	XML	A markup language defines tags (markup) to identify the content, data, and text in XML documents. It differs from HTML , the markup language most often used to present information on the Internet. HTML has fixed tags that deal mainly with style or presentation. An XML document must undergo a transformation into a language with style tags under the control of a style sheet before it can be presented by a browser or other presentation mechanism. Two types of style sheets used with XML are CSS and XSL. Typically, XML is transformed into HTML for presentation. Although tags can be defined as needed in the generation of an XML document, you can use a document type definition (DTD) to

Part 4: Node Guidance

		define the elements allowed in a particular type of document. A document can be compared by using the rules in the DTD to determine its validity and to locate particular elements in the document. A Web services application's J2EE deployment descriptors are expressed in XML with schemas defining allowed elements. Programs for processing XML documents use SAX or DOM APIs. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)
Facade		Provides a unified interface to a set of interfaces in a subsystem. Facade defines a higher-level interface that makes the subsystem easier to use. This can simplify a number of complicated object interactions into a single interface.
Facade Design Pattern		An object that provides a simplified interface to a larger body of code, such as a class library. (Source: http://en.wikipedia.org/wiki/Facade_pattern)
Federated Search		Implementation of a computer program that allows users to access multiple data sources with a single query string located within a single interface. (Source: http://en.wikipedia.org/wiki/Federated_search)
Firewall		A piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy, analogous to the function of firewalls in building construction.
GIG Enterprise Service		A service that provides capabilities for use in the DoD enterprise. GIG Enterprise Services are the combination of Core Enterprise Services and Community of Interest Services. Also referred to as Global Enterprise Services.
Global Command and Control System	GCCS	<p>GCCS-J is the DOD joint C2 system of record for achieving full spectrum dominance. It enhances information superiority and supports the operational concepts of full-dimensional protection and precision engagement. GCCS-J is the principal foundation for dominant battlespace awareness, providing an integrated, near real-time picture of the battlespace necessary to conduct joint and multinational operations. It fuses select C2 capabilities into a comprehensive, interoperable system by exchanging imagery, intelligence, status of forces, and planning information. GCCS-J offers vital connectivity to the systems the joint warfighter uses to plan, execute, and manage military operations.</p> <p>GCCS-J is a Command, Control, Communications, Computer, and Intelligence (C4I) system, consisting of hardware, software, procedures, standards, and interfaces that provide a robust, seamless C2 capability. The system uses the Defense Information Systems Network (DISN) and must work over tactical communication systems to ensure connectivity with deployed forces in the tactical environment. (Source: http://www.disa.mil/gccs-j/)</p>
Global Information Grid	GIG	Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for

Part 4: Node Guidance

		collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.
Global Positioning System		A satellite constellation that provides highly accurate position, velocity, and time navigation information to users. (Source: JP 1-02, http://www.dtic.mil/doctrine/jel/doddict/data/g/02300.html)
High Assurance Internet Protocol Encryption	HAiPE	DoD version of Internet Protocol (IP) security (IPsec) protocol. (Source: http://en.wikipedia.org/wiki/HAiPE)
High Availability		Data tier availability can be affected by hardware failure, power outages, data errors, user errors, programmer errors, OS errors, and RDBMS errors. Various hardware and software methods help mitigate availability issues. The more reliable a system needs to be, the more it costs. Consequently, defining availability to meet requirements is essential to controlling costs.
Horizontal Fusion	HF	Horizontal Fusion (HF) is a direct response to Secretary of Defense Donald H. Rumsfeld's vision of Force Transformation. It demonstrates the ability to use lightweight automation to replace system mass with superior access to information based on a coherent architecture for an arbitrary future. Horizontal Fusion acts as a catalyst by implementing and demonstrating technologies and techniques that significantly advance the process of information-sharing in a an evolving net-centric environment. (Source: http://horizontalfusion.dtic.mil/vision/)
Hypertext Markup Language	HTML	A markup language for hypertext documents on the Internet. HTML supports embedding images, sounds, video streams, form fields, references to other objects with URLs, and basic text formatting. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)
Hypertext Transfer Protocol	HTTP	The Internet protocol used to retrieve hypertext objects from remote hosts. HTTP messages consist of requests from client to server and responses from server to client. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)

Part 4: Node Guidance

Identity Management		Provides the methodology and functions for maintaining information on people, consumers, and service providers. Supports the validation of identity authentication credentials.
Information Assurance	IA	Measures taken to protect and defend our information and information systems to ensure Confidentiality, Integrity, Availability, and Accountability, extended to restoration with protect, detect, monitor, and react capabilities.
Information Support Plan	ISP	The identification and documentation of information needs, infrastructure support, IT and NSS interface requirements and dependencies focusing on net-centric, interoperability, supportability and efficiency concerns. (Source: DoD Instruction 4630.8 , 30 June 2004, [R1168] Enclosure 2, Definitions)
Information Technology	IT	Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Information technology does not include any equipment that is acquired by a federal contractor incidental to a federal contract. (Source: CJCSI 6212.01D, 8 March 2006, Glossary page GL-11)
Information Technology Laboratory	ITL	The ITL at the National Institute of Standards and Technology (NIST) has the broad mission of supporting U.S. industry, government, and academia with measurements and standards that enable new computational methods for scientific inquiry, assure IT innovations for maintaining global leadership, and re-engineer complex societal systems and processes through insertion of advanced Information Technology (IT). (Source: http://www.itl.nist.gov/itl-what_itl_does.html)
Intelligence Community	IC	A federation of executive branch agencies and organizations that conduct intelligence activities necessary for conduct of foreign relations and protection of national security. (Source: http://www.intelligence.gov/)

Part 4: Node Guidance

Interface		The functional and physical characteristics required to exist at a common boundary or connection between systems or items. (Source: DoD 4120.214-M)
Internet		The Internet, or simply the Net, is the publicly available worldwide system of interconnected computer networks that transmit data by packet switching using a standardized Internet Protocol (IP) and many other protocols. It is made up of thousands of smaller commercial, academic, and government networks. It carries various information and services, such as electronic mail, online chat and the interlinked web pages and other documents of the World Wide Web. Because this is by far the largest, most extensive internet (with a lower case i) in the world, it is simply called the Internet (with a capital I). (Source: http://en.wikipedia.org/wiki/Internet)
Internet Engineering Task Force	IETF	The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. (Source: http://www.ietf.org/overview.html)
Internet Protocol	IP	Data packets routed across network, not switched via dedicated circuits.
Internet Protocol Version 4	IPv4	Version 4 of the Internet Protocol (IP). It was the first version of the Internet Protocol to be widely deployed, and forms the basis for most of the current Internet (as of 2004). It is described in IETF RFC 791, which was first published in September, 1981. IPv4 uses 32-bit addresses, limiting it to 4,294,967,296 unique addresses, many of which are reserved for special purposes such as local networks or multicast addresses. This reduces the number of addresses that can be allocated as public Internet addresses. As the number of addresses available is consumed, an IPv4 address shortage appears to be inevitable in the long run. This limitation has helped stimulate the push towards IPv6, which is currently in the early stages of deployment, and may eventually replace IPv4. (Source: http://en.wikipedia.org/wiki/IPv4)
Internet Protocol Version 6	IPv6	Version 6 of the Internet Protocol; it was initially called IP Next Generation (IPng) when it was picked as the winner in the IETF's IPng selection process. IPv6 is intended to replace the previous standard, IPv4, which only supports up to about 4 billion (4×10^9) addresses. IPv6 supports up to about 3.4×10^{38} (340 undecillion) addresses. This is the equivalent of 4.3×10^{20} (430 quintillion) addresses per square inch (6.7×10^{17} (670 quadrillion) addresses/mm ²) of the Earth's surface. It is expected that IPv4 will be supported until at least 2025, to allow time for bugs and system errors to be corrected. (Source: http://en.wikipedia.org/wiki/Ipv6)
Intrusion Detection System	IDS	An IDS inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or

Part 4: Node Guidance

		compromise a system. (Source: http://www.webopedia.com/TERM/i/intrusion_detection_system.html)
Java 2 Platform, Enterprise Edition	J2EE	The J2EE environment is the standard for developing component-based multi-tier enterprise applications. The J2EE platform consists of a set of services, application programming interfaces (APIs), and protocols that provide the functionality for developing multitiered, Web-based applications. Features include Web services support and development tools. Sun Microsystems has simplified the name of the Java platform for the enterprise; the "2" is dropped from the name, as well as the dot number so the next version of the Java platform for the enterprise is Java Platform, Enterprise Edition 5 or Java EE 5. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)
Java Platform, Enterprise Edition	Java EE	<p>Java Platform, Enterprise Edition (Java EE) is the industry standard for developing portable, robust, scalable and secure server-side Java applications. Building on the solid foundation of the Java Platform, Standard Edition (Java SE), Java EE provides Web services, component model, management, and communications APIs that make it the industry standard for implementing enterprise-class service-oriented architecture (SOA) and next-generation Web applications.</p> <p>Sun Microsystems has simplified the name of the Java platform for the enterprise. Formerly, the platform was known as Java 2 Platform, Enterprise Edition (J2EE), and specific versions had "dot numbers" such as J2EE 1.4. The "2" is dropped from the name, as well as the dot number so the next version of the Java platform for the enterprise is Java Platform, Enterprise Edition 5 or Java EE 5. (Source: http://java.sun.com/javaee/)</p>
JavaScript		The Netscape-developed object scripting language used in millions of web pages and server applications worldwide. Contrary to popular misconception, JavaScript is not "Interpretive Java." Rather, it is a dynamic scripting language that supports prototype-based object construction.
JavaServer Page	JSP	An extensible Web technology that uses static data, JSP elements, and server-side Java objects to generate dynamic content for a client. Typically the static data is HTML or XML elements, and in many cases the client is a Web browser. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)
Java Specification Request	JSR	
Joint Capabilities Integration and Development System	JCIDS	Establishes procedures to support the Chairman of the Joint Chiefs of Staff and the Joint Requirements Oversight Council (JROC) in identifying, assessing and prioritizing joint military capability. (Source: CJCSI 3170.01E, 11 May 2005, <i>Joint Capabilities Integration and Development System</i>)
Joint Interoperability Test Command	JITC	Independent operational test and evaluation/assessor of DISA and other DoD Command, Control, Communications, Computers and Intelligence (C4I) acquisitions. (Source: http://jitic.fhu.disa.mil/mission.htm)

Part 4: Node Guidance

Joint Worldwide Intelligence Communications System	JWICS	The sensitive, compartmented information portion of the Defense Information Systems Network . It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. (Source: http://www.dtic.mil/doctrine/jel/doddict/data/j/02972.html)
Key Interface Profile	KIP	An operational functionality, systems functionality and technical specifications description of the Key Interface. The profile consists of refined Operational and Systems Views, interface control specifications, Technical View with SV-TV Bridge, and referenced procedures for KIP compliance. The key interface profile is the technical specification that governs access to the GIG . (Source: CJCSI 6212.01D, 8 March 2006, Glossary page GL-14)
Key Performance Parameters	KPP	Those attributes or characteristics of a system that are considered critical or essential to the development of an effective military capability and those attributes that make a significant contribution to the key characteristics as defined in the Joint Operations Concepts. KPPs are validated by the Joint Requirements Oversight Council (JROC) for JROC Interest documents, and by the DOD component for Joint Integration or Independent documents. Capability development and capability production document KPPs are included verbatim in the acquisition program baseline. (Source: CJCSI 3170.01E. <i>Joint Capabilities and Development System</i> , 11 May 2005, Glossary page GL-12)
Least-Common-Denominator Data Access Mechanism		When one application is able to obtain data provided by another by removing arbitrary implementation barriers to data exchange.
Legacy System		An existing computer system or application program which continues to be used because the user (typically an organization) does not want to replace or redesign it. (Source: http://en.wikipedia.org/wiki/Legacy_system)
Link-16	TADIL-J	Tactical Data Information Link (TADIL) primarily designed for use by Command and Control (C2) and Air-to-Air assets; uses the Joint Tactical Data Link (TADIL-J) message format. (Source: http://aatc.aztucs.ang.af.mil/aatcinfo.htm)
Local Area Network	LAN	A group of interconnected computer and support devices. (Source: http://www.sun.com/products-n-solutions/hardware/docs/html/817-6210-10/glossary.html)

Part 4: Node Guidance

Machine-to-Machine Messaging		Provides reliable machine-to-machine message exchange across the enterprise .										
Mediation		<p>A set of negotiated agreements for interacting between components that enable those components to work together to perform a task. These agreements are defined through standard interfaces and data interchange specifications.</p> <p>Mediation services provide multiple methods for integrating data sources and services:</p> <table border="1"> <tr> <td>Transformation</td> <td>When a client requests a particular format, a transformer converts the data before returning it.</td> </tr> <tr> <td>Aggregation</td> <td>A mediator service may aggregate data from multiple sources, thus acting as a single source. There may be one or more sources.</td> </tr> <tr> <td>Adaptation</td> <td>When a client cannot connect to a service, an adapter provides a different transport protocol as well as a different data format. The need to communicate is the same.</td> </tr> <tr> <td>Orchestration</td> <td>Co-ordination of events and tasks. It directs and manages the flow of data between multiple component services in an application or business process.</td> </tr> <tr> <td>Choreography</td> <td>When a client requests a service, a choreographer or service requests that other services when to execute other services. It defines when services to interact; When a business process manager implements choreography.</td> </tr> </table>	Transformation	When a client requests a particular format, a transformer converts the data before returning it.	Aggregation	A mediator service may aggregate data from multiple sources, thus acting as a single source. There may be one or more sources.	Adaptation	When a client cannot connect to a service, an adapter provides a different transport protocol as well as a different data format. The need to communicate is the same.	Orchestration	Co-ordination of events and tasks. It directs and manages the flow of data between multiple component services in an application or business process.	Choreography	When a client requests a service, a choreographer or service requests that other services when to execute other services. It defines when services to interact; When a business process manager implements choreography.
Transformation	When a client requests a particular format, a transformer converts the data before returning it.											
Aggregation	A mediator service may aggregate data from multiple sources, thus acting as a single source. There may be one or more sources.											
Adaptation	When a client cannot connect to a service, an adapter provides a different transport protocol as well as a different data format. The need to communicate is the same.											
Orchestration	Co-ordination of events and tasks. It directs and manages the flow of data between multiple component services in an application or business process.											
Choreography	When a client requests a service, a choreographer or service requests that other services when to execute other services. It defines when services to interact; When a business process manager implements choreography.											
Metadata		Data about the data, that is, the description of the data resources, its characteristics, location, usage, and so on. Metadata is used to identify, describe, and define user data.										
Modular Design		Characterized by (1) Functional partitioning into discrete, scalable, reusable modules consisting of isolated, self-contained functional elements; (2) Rigorous use of well-defined modular interfaces, including object-oriented descriptions of module functionality; (3) Ease of change to achieve technology transparency and, to the extent possible, make use of industry standards for key interfaces.										
Multicast		The delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once and only create copies when the links to the destinations split. (Source: http://en.wikipedia.org/wiki/Multicast)										
MX Record		An MX record or Mail exchanger record is a type of resource record in the Domain Name System (DNS) specifying how Internet e-mail should be routed. MX records point to the servers that should receive an e-mail, and their priority relative to each other. (Source: http://en.wikipedia.org/wiki/MX_Record)										

Part 4: Node Guidance

Namespace		<p>A namespace is an abstract container which contains a logical grouping of unique identifiers (i.e., names). An identifier defined in a namespace is associated with that namespace. It is possible to define the same identifier independently in multiple namespaces. That is, the meaning associated with an identifier defined in one namespace may or may not have the same meaning as the same identifier defined in another namespace. Languages that support namespaces specify the rules that determine to which namespace an identifier (i.e., not its definition) belongs. (Adapted from: http://en.wikipedia.org/wiki/Namespace_%28computer_science%29; accessed 2/6/2008)</p> <p>XML namespaces provide a simple method for qualifying element and attribute names used in Extensible Markup Language documents by associating them with namespaces identified by URI references. (Source http://www.w3.org/TR/REC-xml-names/)</p>
National Institute of Standards and Technology	NIST	<p>Non-regulatory federal agency within the U.S. Commerce Department's Technology Administration with a mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. (Source: http://www.nist.gov/public_affairs/general2.htm)</p>
National Security Agency	NSA	<p>America's cryptologic organization; it coordinates, directs, and performs highly specialized activities to protect U.S. government information systems and produce foreign signals intelligence information. (Source: http://www.nsa.gov/about/index.cfm)</p>
National Security Systems	NSS	<p>Telecommunications and information systems, operated by the Department of Defense, the functions, operation, or use of which involves: (1) intelligence activities; (2) cryptologic activities related to national security; (3) the command and control of military forces; (4) equipment that is an integral part of a weapon or weapons systems; or (5) is critical to the direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Source: CJCSI 3170.01F, 1 May 2007, page GL-16)</p>
Net-Centric Enterprise Services	NCES	<p>The NCES program provides enterprise-level Information Technology (IT) services and infrastructure components, also called Core Enterprise Services, for the Department of Defense (DoD) Global Information Grid (GIG).</p>
Net-Centric Enterprise Solutions for Interoperability	NESI	<p>A cross service effort between the U.S. Navy Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I), the U.S. Air Force Electronic Systems Center (ESC) and the Defense Information Systems Agency (DISA). NESI provides a reference architecture, implementation guidance, and a set</p>

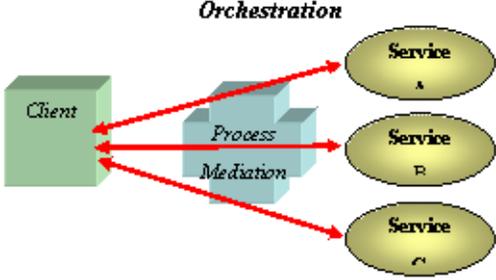
Part 4: Node Guidance

		of reusable software components. These facilitate the design, development, maintenance, evolution, and use of information systems for the Net-Centric Operations and Warfare (NCOW) environment.
Net-Centric Operations and Warfare Reference Model	NCOW RM	The NCOW RM describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic userinterface, the intelligent-assistant capabilities, the net-centric service capabilities (core services, Community of Interest (COI) services , and environment control services), and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the Global Information Grid (GIG) are realized. The NCOW RM represents the objective end-state for the GIG. This objective end-state is a service-oriented, inter-networked, information infrastructure in which users request and receive services that enable operational capabilities across the range of military operations; DoD business operations; and Department-wide enterprise management operations. The NCOW RM is a key compliance mechanism for evaluating DoD information technology capabilities and the Net-Ready Key Performance Parameter . (Source: CJCSI 6212.01D, 8 March 2006, Glossary pages GL-17 and GL-18)
Net-Ready Key Performance Parameter	NR-KPP	<p>The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following elements:</p> <ul style="list-style-type: none"> • Compliance with the NCOW RM. • Compliance with applicable GIG KIPs. • Verification of compliance with DoD information assurance requirements. • Supporting integrated architecture products required to assess information exchange and use for a given capability. <p>(Source: DoD Instruction 4630.8, <i>Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)</i>, 30 June 2004, [R1168] Enclosure 2 Section E2.1.51)</p>
Network Intrusion Detection	NID	Attempt to detect malicious activity such as denial of service attacks, port-scans or even attempts to crack into computers by monitoring network traffic. (Source: http://en.wikipedia.org/wiki/Network_intrusion-detection_system)

Part 4: Node Guidance

Network Operations	NetOps	<p>An organizational, procedural, and technological construct for ensuring information and decision superiority at the strategic, operational, and tactical levels of warfare as well as within DoD business operations. NetOps is an operational approach, which addresses the interdependency and integration of IA/CND, S&NM, and CS capabilities. NetOps consists of the organizations, tactics, techniques, procedures, functionalities, and technologies required to plan, administer, and monitor use of the GIG infrastructure and the end-to-end information flows of the GIG; and to respond to threats, outages, and other operational impact. NetOps ensures mission requirements are properly considered in GIG operational decision-making. NetOps enables the GIG to provide its users with information they need, when and where they need it, with appropriate protection. NetOps is essential for successful execution of net-centric warfare and other net-centric operations in support of national security objectives.</p>
Network Time Protocol	NTP	<p>Protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses User Datagram Protocol (UDP) port 123 as its transport layer. It is designed particularly to resist the effects of variable latency. (Source: http://en.wikipedia.org/wiki/Network_Time_Protocol)</p>
Node		<p>In general network usage, a node is a processing location such as a computer or some other device. Every node has a unique network address, sometimes called a Data Link Control (DLC) address or Media Access Control (MAC) address. (Source: http://www.webopedia.com/TERM/n/node.html)</p> <p>A NESI Node is a collection of integrated components (i.e., systems, applications, services and other Nodes) that are bound together spatially and/or temporally to meet the needs of a particular mission. It is conceptual in nature and can not be defined in terms of a concrete set of components or size. The membership of a component within a particular Node is not exclusive and a Component can be part of multiple Nodes.</p>
Node Information Services	NIS	
Online Certificate Status Protocol	OCSP	<p>Online Certificate Status Protocol is a method for determining the revocation status of an X.509 digital certificate using means other than CRLs. It is described in RFC 2560 and is on the Internet standards track.</p> <p>OCSP messages are encoded in ASN.1 and usually communicated over HTTP. OCSP's request/response nature leads to OCSP servers being termed as OCSP responders.</p>
Operational View	OV	<p>The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions. DoD missions include both warfighting missions and business processes. The OV contains graphical and textual products that comprise an identification of the operational nodes and elements, assigned tasks and activities, and information flows required between nodes. It</p>

Part 4: Node Guidance

		<p>defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges. (Source: <i>DoDAF v1.5 Volume I: Definitions and Guidelines</i>, 23 April 2007)</p>
<p>Orchestration</p>		<p>Co-ordination of events in a process; orchestration directs and manages the on-demand assembly of multiple component services to create a composite application or business process. (Source: http://looselycoupled.com/glossary/orchestration)</p>  <p>11164</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: See <i>Mediation</i>.</p> </div>
<p>Plain Text</p>	<p>PT See</p>	

Part 4: Node Guidance

Plug-In		A hardware or software module that adds a specific feature or service to a larger system. (Source: http://www.webopedia.com/TERM/p/plug_in.html)
Portal		A Web portal is a Web site that provides a starting point, gateway, or portal to other resources on the Internet or an intranet. Intranet portals are also known as "enterprise information portals" (EIP). Examples of existing portals are Yahoo, Excite, Lycos, Altavista, Infoseek, and Hotbot. (Source: http://en.wikipedia.org/wiki/web_portal)
Portlet		A reusable Web component that displays relevant information to portal users. Examples for portlets include email, weather, discussion forums, and news. The purpose of the Web Services for Remote Portlets (WSRP) interface is to provide a Web services standard that allows for the "plug-n-play" of portals , other intermediary Web applications that aggregate content, and applications from disparate sources. The portlet specification enables interoperability between portlets and portals. This specification defines a set of APIs for portal computing that addresses the areas of aggregation, personalization, presentation, and security. (Source: http://en.wikipedia.org/wiki/Portlets)
Protocol		An agreed-upon format for transmitting data between two devices. The protocol determines the type of error checking to be used, data compression method, if any, how the sending device will indicate that it has finished sending a message, and how the receiving device will indicate that it has received a message. (Source: http://www.webopedia.com/TERM/p/protocol.html)
Proxy		A server that sits between a client application, such as a Web browser , and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. Proxy servers have two main purposes: improve performance and filter requests. (Source: http://www.webopedia.com/TERM/p/proxy_server.html)
Public Key	PK	See Public Key Cryptography .
Public Key Cryptography		Public key cryptography, also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys - a public key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key. (Source: http://en.wikipedia.org/wiki/Public_key)
Public Key Enabling	PK-Enabling	The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and nonrepudiation. PK-Enabling involves replacing existing

Part 4: Node Guidance

		or creating new user authentication systems using certificates instead of other technologies, such as userid and password or Internet Protocol filtering; implementing public key technology to digitally sign, in a legally enforceable manner, transactions and documents; or using public key technology, generally in conjunction with standard symmetric encryption technology, to encrypt information at rest and/or in transit. (Source: DoD Instruction 8520.2, <i>Public Key Infrastructure (PKI) and Public Key (PK) Enabling</i> , 1 April 2004 [R1206])
Public Key Infrastructure	PKI	Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. (Source: CNSS Instruction No. 4009, Revised May 2003, <i>National Information Assurance (IA) Glossary</i>)
Quality of Service	QoS	Data timeliness, accuracy, completeness, integrity, and ease of use. Refers to the probability of the network meeting a given traffic contract. In many cases is used informally to refer to the probability of a packet passing between two points in the network. (Source: http://en.wikipedia.org/wiki/Quality_of_service) -OR- A defined level of performance that adapts to the environment in which it is operating. QoS may be requested by the user of the information. The level of QoS provided is based on the request, the available capabilities of the provider, and the priority of the user.
Reference Data Set		The Reference Data Set Gallery [of the DoD Metadata Registry and Clearinghouse] provides collections of related data that represent a defined entity within a community of interest. Examples of reference data sets include country codes, U.S. state codes, and marital status codes. (Source: http://www.disa.mil/nces/development/developer_doc_overview.html)
Registered Namespace		A namespace that has been registered and approved with a namespace registration services. For the DoD, use the DoD Metadata Registry .
Registration Web Service	RWS	Horizontal Fusion (HF) service used by data producers to register content sources.
Relational Database	RDB	A collection of data items organized as a set of formally-described tables from which data can be accessed or reassembled in many different ways without having to reorganize the database tables.
Role-Based Access Control	RBAC	An approach to restricting system access to authorized users. It is a newer and alternative approach to discretionary access control and mandatory access control. It assigns permissions to specific operations with meaning in the organization, rather than to low-level data objects. (Source: http://en.wikipedia.org/wiki/RBAC)

Part 4: Node Guidance

Router		A device that forwards data packets along networks. A router is connected to at least two networks, commonly two local area networks (LANs) or wide area networks (WANs) or a LAN and its Internet Service Provider's network. Routers are located at gateways, the places where two or more networks connect. (Source: http://www.webopedia.com/TERM/r/router.html)
Schema		A diagrammatic representation, an outline, or a model. In relation to data management, a schema can represent any generic model or structure that deals with the organization, format, structure, or relationship of data. Some examples of schemas are (1) a database table and relational structure, (2) a document type definition (DTD), (3) a data structure used to pass information between systems, and (4) an XML schema document (XSD) that represents a data structure and related information encoded as XML. Schemas typically do not contain information specific to a particular instance of data (Source: DoD 8320.02-G , 12 April 2006, <i>Guidance for Implementing Net-Centric Data Sharing</i>)
Search Web Service	SWS	Horizontal Fusion (HF) service used to search for content from registered sources.
Secret Internet Protocol Router Network	SIPRNet	DoD's largest interoperable command and control data network, supporting the Global Command and Control System (GCCS), the Defense Message System (DMS), collaborative planning and numerous other classified warfighter applications. Direct connection data rates range from 56 kbps to 155 Mbps for the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet), and up to 45 Mbps for the SIPRNet. Remote dial-up services are also available, ranging from 19.2 kbps on SIPRNet to 56 kbps on NIPRNet. (Source: http://www.disa.mil/main/prodsol/data.html)
Security Technical Implementation Guide	STIG	Configuration standards for DoD IA and IA-enabled devices/systems. (Source: http://iase.disa.mil/stigs/index.html)
Sensitive Compartmented Information	SCI	Classified information concerning or derived from intelligence sources, methods, or analytical processes, that is required to be handled within formal access control systems established by the Director of Central Intelligence (DCI). (Source: DoDD 8520.1 , 20 December 2001, <i>Protection of Sensitive Compartmented Information (SCI)</i> , Page 2, Section 3.3)

Part 4: Node Guidance

Server		A computer software application that carries out some task (i.e., provides a service) on behalf of yet another piece of software called a client .
Service		A service is an autonomous encapsulation of some business or mission functionality. The service concept includes the notion of service providers and service consumers interacting via well-defined reusable interfaces. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: See P1304: Service-Oriented Architecture in Part 1 for additional information concerning services including implementation characteristics.</p> </div>
Service Access Point	SAP	SAP provides all of the information necessary for a user to access and consume a service. Includes the logical and physical location of the service on the net.
Service Definition Framework	SDF	SDF provides service users, customers, developers, providers, and managers with a common frame of reference. Its structure and methodology enable you to fully define the Service Access Points (SAPs) for the service.
Service Discovery	SD	Provides a yellow pages , categorized by DoD function, enabling users to advertise and locate capabilities available on the network.
Service Level Agreement	SLA	A contractual vehicle between a service provider and a service consumer. It specifies performance requirements, measures of effectiveness, reporting, cost, and recourse. It usually defines repair turnaround times for users.
Service Management		Enables monitoring of DoD Web services . Provides reporting of service-level information to potential and current service consumers, program analysts, and program managers.
Service-Oriented Architecture	SOA	NESI describes SOA as an architectural style used to design, develop, and deploy information technology (IT) systems based on decomposing functionality into services with well-defined interfaces. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: See P1304: Service-Oriented Architecture in Part 1 for additional information.</p> </div>
Situation Awareness Data Link	SADL	An Enhanced Position Location and Reporting System (EPLRS) radio modified for use in an aircraft. SADL and EPLRS radios are used to establish a common secure tactical data link network. (Source: http://aatc.aztuks.ang.af.mil/aatcinfo.htm)

Part 4: Node Guidance

Smart Card		<p>A credit card-size device, normally for carrying and use by personnel, that contains one or more integrated circuits and also may employ one or more of the following technologies: magnetic stripe, bar codes (linear and two-dimensional), non-contact and radio frequency transmitters, biometric information, encryption and authentication, or photo identification. (Source: DoDD 8190.3, <i>Smart Card Technology</i>, 31 August 2003, Page 2, Section 3.2)</p>
SOAP		<p>SOAP Version 1.2 is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. It uses XML technologies to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation specific semantics. (Source: SOAP Version 1.2 Second Edition, http://www.w3.org/TR/soap12-part1/#intro)</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: <i>The World Wide Web Consortium (W3C) changed the name of this protocol from Simple Object Access Protocol 1.1 (SOAP) to SOAP Version 1.2 in the current version.</i></p> </div>
Software Component		<p>A software component is a software system element offering a predefined service and able to communicate with other components. It is a unit of independent deployment and versioning, encapsulated, multiple-use, non-context-specific and composable with other components.</p> <p>Source: http://en.wikipedia.org/wiki/Software_component#Software_component</p>
Software Developers Kit	SDK	<p>A set of development tools that allows a software engineer to create applications for a certain software package, software framework, hardware platform, computer system, operating system, and so on. It may be as simple as an application programming interface in the form of some files to interface to a particular programming language, or as complex as sophisticated hardware to communicate with a certain embedded system. Common tools include debugging aids and other utilities. SDKs frequently include sample code, technical notes, and other supporting documentation to clarify points from the primary reference material. (Source: http://en.wikipedia.org/wiki/SDK)</p>
Software Product Line	SPL	<p>A software product line (SPL) is a set of software-intensive systems that share a common, managed set of features satisfying the specific needs of a particular market segment or mission and that are developed from a common set of core assets in a prescribed way. (Source: Software Engineering Institute)</p>

Part 4: Node Guidance

Spyware		Any software that covertly gathers user information through the user's Internet connection without the user's knowledge, usually for advertising purposes. (Source: http://www.webopedia.com/TERM/s/spyware.html)
Stakeholder		An enterprise, organization, or individual having an interest or a stake in the outcome of the engineering of a system. (Source: EIA-632, Annex A)
Storage		Provides physical and virtual places to host and retain data for purposes such as content staging, continuity of operations, or archival.
Sustainment		One of the two major efforts (with disposal) of the Operations and Support phase of a DoD acquisition program. Sustainment includes supply, maintenance, transportation, sustaining engineering, data management, configuration management, manpower, personnel, training, habitability, survivability, environment, safety (including explosives safety), occupational health, protection of critical program information, anti-tamper provisions, and Information Technology (IT), including National Security Systems (NSS), supportability and interoperability functions. (Source: DoD Instruction 5000.2 , 12 May 2003, <i>Operation of the Defense Acquisition System</i> , Section 3.9.2)
System		Two or more interrelated pieces of equipment (or sets) arranged in a package to perform an operational function or to satisfy a requirement. (Source: <i>Defense Acquisition Glossary of Terms</i> , Jan 2001)
System Component		<p>A basic part of a system. System components may be personnel, hardware, software, facilities, data, material, services, and/or techniques that satisfy one or more requirements in the lowest levels of the functional architecture. System components may be subsystems and/or configuration items.</p> <div data-bbox="711 1318 1372 1381" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: See component.</p> </div>
Systems and Services View	SV	The SV is a set of graphical and textual products that describes systems and interconnections providing for, or supporting, DoD functions. DoD functions include both warfighting and business functions. The SV associates systems resources to the Operational View (OV). These systems resources support the operational activities and facilitate the exchange of information among operational nodes. (Source: DoDAF v1.5 Volume I: Definitions and Guidelines , 23 April 2007)

Part 4: Node Guidance

Taxonomy		The science of categorization, or classification, of things based on a predetermined system. In reference to Web sites and portals, a site's taxonomy is the way it organizes its data into categories and subcategories, sometimes displayed in a site map. (Source: http://www.webopedia.com/TERM/t/taxonomy.html)
Taxonomy Gallery		The Taxonomy Gallery [of the DoD Metadata Registry and Clearinghouse] provides XML-based taxonomy files that describe one or more nodes in a hierarchical classification of items, and their relationships to other nodes. The taxonomy files registered with the Taxonomy Gallery are organized by governance namespace. (Source: http://www.disa.mil/nces/development/developer_doc_overview.html)
Technical Standards View	TV	The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements. Its purpose is to ensure that a system satisfies a specified set of operational requirements. The TV provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The TV includes a collection of the technical standards, implementation conventions, standards options, rules, and criteria organized into profile(s) that govern systems and system elements for a given architecture. (Source: <i>DoDAF v1.5 Volume 1: Definitions and Guidelines</i> , 23 April 2007)
Test and Evaluation Master Plan	TEMP	Describes all planned testing, including measures to evaluate the performance of the system during test periods, an integrated test schedule, and resource requirements.
Topic		<p>Topics are used to manage content flow between publishers and subscribers. Topics must be known in such a way that subscribers can refer to them unambiguously.</p> <p>In DDS, Topics conceptually fits between publications and subscriptions and associate a name (unique in the domain), a data-type, and QoS parameters related to the data.</p>
Transmission Control Protocol	TCP	One of the core protocols of the Internet protocol suite. Using TCP, programs on networked computers can create connections to one another, over which they can send data. The protocol guarantees that data sent by one endpoint will be received in the same order by the other, without any pieces missing. It also distinguishes data for different applications (such as a Web server and an email server) on the same computer. (Source: http://en.wikipedia.org/wiki/Transmission_Control_Protocol)
Transmission Control Protocol/Internet Protocol	TCP/IP	A suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols, such as Netware, also support TCP/IP.

Part 4: Node Guidance

Trusted Guard		Accredited to pass information between two networks at different security levels according to well defined rules and other controls. Guard products only pass defined types of information (e.g., email, images, or formatted messages). A key challenge is how to implement net-centric operations across trusted guards in the presence of CES services.
Unclassified but Sensitive Internet Protocol Router Network	NIPRNet	NIPRNet provides seamless interoperability for unclassified combat support applications, as well as controlled access to the Internet. Direct connection data rates range from 56Kbps to 622Mbps. Remote dial-up services are available up to 56Kbps. (Source: http://www.disa.mil/main/prodsol/data.html)
Uniform Resource Identifier	URI	An encoded address that represents any Web resource, such as an HTML document, image, video clip, or program. As opposed to a URL or a URN , which are concrete entities, a URI is an abstract superclass. (Source: http://publib.boulder.ibm.com/infocenter/adiehelp/index.jsp?topic=/com.ibm.wsinted.glossary.doc/topics/glossary.html)
Uniform Resource Locator	URL	A sequence of characters that represents information resources on a computer or in a network such as the Internet. This sequence of characters includes (1) the abbreviated name of the protocol used to access the information resource and (2) the information used by the protocol to locate the information resource. (Source: http://publib.boulder.ibm.com/infocenter/adiehelp/index.jsp?topic=/com.ibm.wsinted.glossary.doc/topics/glossary.html)
Uniform Resource Name	URN	A name that uniquely identifies a Web service to a client . (Source: http://publib.boulder.ibm.com/infocenter/adiehelp/index.jsp?topic=/com.ibm.wsinted.glossary.doc/topics/glossary.html)
Universal Description, Discovery, and Integration	UDDI	An industry initiative to create a platform-independent, open framework for describing services, discovering businesses, and integrating business services using the Internet, as well as a registry. It is being developed by a vendor consortium. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)
User Datagram Protocol		

Part 4: Node Guidance

Web Application		A collection of components that can be bundled together and run in multiple containers from multiple vendors. -OR- An application written for the Internet, including those built with Java technologies such as Java Server Pages and servlets, and those built with non-Java technologies such as CGI and Perl. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)
Web Browser		A client program that initiates requests to a Web server and displays the information that the server returns. (Source: http://publib.boulder.ibm.com/infocenter/adiehelp/index.jsp?topic=/com.ibm.wsinted.glossary.doc/topics/glossary.html)
Web Container		A container that implements the Web-component contract of the J2EE architecture. This contract specifies a runtime environment for Web components that includes security, concurrency, life-cycle management, transaction, deployment, and other services. A Web container provides the same services as a JSP container as well as a federated view of the J2EE platform APIs . A Web container is provided by a Web or J2EE server. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)
Web Server		Software that provides services to access the Internet, an intranet, or an extranet. A Web server hosts Web sites , provides support for HTTP and other protocols, and executes server-side programs (such as CGI scripts or servlets) that perform certain functions. In the J2EE architecture, a Web server provides services to a Web container . For example, a Web container typically relies on a Web server to provide HTTP message handling. The J2EE architecture assumes that a Web container is hosted by a Web server from the same vendor, so it does not specify the contract between these two entities. A Web server can host one or more Web containers. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)
Web Service		A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards. (Source: http://www.w3.org/TR/ws-gloss/)
Web Services Description Language	WSDL	WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. (Source: W3C Note on WSDL 1.1 of 15 March 2001 http://www.w3.org/TR/wsdl)
Web Services for Interactive Applications	WSIA	
Web Services for Remote Portlets	WSRP	The WSRP specification defines a Web service interface for interacting with interactive presentation-oriented Web

Part 4: Node Guidance

		<p>services. It has been produced through the joint efforts of the Web Services for Interactive Applications (WSIA) and Web Services for Remote Portals (WSRP) OASIS Technical Committees. Scenarios that motivate WSRP/WSIA functionality include (1) portal servers providing portlets as presentation-oriented Web services that can be used by aggregation engines; (2) portal servers consuming presentation-oriented Web services provided by portal or non-portal content providers and integrating them into a portal framework. (Source: http://www.oasis-open.org/committees/download.php/3343/oasis-200304-wsrp-specification-1.0.pdf)</p>
Web Services Interoperability Organization	WS-I	<p>WS-I is an open industry organization chartered to promote Web services interoperability across platforms, operating systems and programming languages. The organization's diverse community of Web services leaders helps customers to develop interoperable Web services by providing guidance, recommended practices and supporting resources. (Source: http://www.ws-i.org/about/Default.aspx)</p>
Web Site		<p>A Web site, website, or WWW site (often shortened to just "site") is a collection of Web pages (i.e., HTML/XHTML documents accessible via HTTP on the Internet). All publicly accessible Web sites in existence comprise the World Wide Web. The pages of a Web site are accessed from a common root URL, the homepage, and usually reside on the same physical server. The URLs of the pages organize them into a hierarchy, although the hyperlinks between them control how the reader perceives the overall structure and how the traffic flows between the different parts of the site. (Source: http://en.wikipedia.org/wiki/web_site)</p>
World Wide Web	WWW	<p>The World Wide Web ("WWW," or simply "Web") is an information space in which items of interest, referred to as resources, are identified by global identifiers called Uniform Resource Identifiers (URI). The term is often mistakenly used as a synonym for the Internet, but the web is actually a service that operates over the Internet. (Source: http://en.wikipedia.org/wiki/World_Wide_web)</p>
World Wide Web Consortium	W3C	<p>The World Wide Web Consortium (W3C) is an international consortium where Member organizations, a full-time staff, and the public work together to develop Web standards. W3C's mission is to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web. (Source: http://www.w3.org/Consortium/)</p>

Part 4: Node Guidance

XML Gallery		The XML Gallery [of the DoD Metadata Registry and Clearinghouse] contains information resources such as submission packages, elements, attributes, and schemas that have been registered by DOD software developers. These information resources use XML, a platform and vendor independent format for exchanging data, to handle data, data structures, and data descriptions (metadata). (Source: http://www.disa.mil/nces/development/developer_doc_overview.html)
XML Information Resources		Document Type Definition (DTD) or XML Schema Documents (XSD) files.
XML Schema Definition	XSD	A language proposed by the W3C XML Schema Working Group for use in defining schemas. Schemas are useful for enforcing structure and/or constraining the types of data that can be used validly within other XML documents. XML Schema Definition refers to the fully specified and currently recommended standard for use in authoring XML schemas. Because the XSD specification was only recently finalized, support for it was only made available with the release of MSXML 4.0. It carries out the same basic tasks as DTD, but with more power and flexibility. Unlike DTD, which requires its own language and syntax, XSD uses XML syntax for its language. XSD closely resembles and extends the capabilities of XDR. Unlike XDR, which was implemented and made available by Microsoft in MSXML 2.0 and later releases, the W3C now recommends the use of XSD as a standard for defining XML schemas. (Source: http://msdn2.microsoft.com/en-us/library/ms256452.aspx)
XSL Transformations	XSLT	A language to express the transformation of XML documents into other XML documents. (Source: W3C Glossary)

References

R1164	DoD Directive 5000.1, <i>The Defense Acquisition System</i> , 12 May 2003 (certified current as of 24 November 2003); http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf .
R1165	DoD Instruction 5000.2, <i>Operation of the Defense Acquisition System</i> , 12 May 2003; http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf .
R1168	DoD Instruction 4630.8, <i>Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)</i> , 30 June 2004; http://www.dtic.mil/whs/directives/corres/pdf/463008p.pdf .
R1172	<i>DoD Net-Centric Data Strategy</i> , DoD Chief Information Officer, 9 May 2003, http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf .
R1176	<i>Net-Centric Operations and Warfare Reference Model (NCOW RM)</i> , v1.1, 17 November 2005.
R1177	<i>Net-Centric Checklist</i> , V2.1.3, Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, 12 May 2004; http://www.defenselink.mil/cio-nii/docs/NetCentric_Checklist_v2-1-3_.pdf .
R1179	<i>DoD IT Standards Registry (DISR)</i> ; http://disronline.disa.mil .
R1181	<i>Global Information Grid (GIG) Key Interface Profiles (KIPs) Framework (DRAFT)</i> , Version 0.95, 7 October 2005.
R1190	DoD CIO memos: <ul style="list-style-type: none"> • 9 June 2003, <i>Internet Protocol Version 6 (IPv6)</i> • 29 September 2003, <i>Internet Protocol Version 6 (Ipv6) Interim Transition Guidance</i> • 28 November 2003, <i>Internet Protocol Version 6 (IPv6) Transition Plan Coordination and Interim Tasking</i> • 16 August 2005, <i>Internet Protocol Version 6 (Ipv6) Policy Update</i> • 16 August 2005, <i>DoD Internet Protocol Version 6 (IPv6) Pilot Nominations</i>
R1191	DoD Directive O-8530.1, <i>Computer Network Defense</i>
R1192	DoD Instruction O-8530.2, <i>Support to Computer Network Defense Services (CNDS)</i>
R1193	See the following items from the Defense Acquisition Guidebook: <ul style="list-style-type: none"> • Compliance with the Net-Centric Operations and Warfare Reference Model • Compliance with Applicable Global Information Grid Key Interface Profiles • Compliance with DoD Information Assurance Requirements • Supporting Integrated Prchitecture Products
R1194	DoD Directive 5000.1, Enclosure 1, Paragraph E1.9, Information Assurance

Part 4: Node Guidance

	Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide information to other DoD systems. DoD policy for information assurance of information technology, including NSS, appears in DoD Directive 8500.1.
R1195	<p>DoD Instruction 5000.2, Enclosure 4, Paragraph E.4.2, IT System Procedures <i>The program defines the requirement for an Information Assurance Strategy for Mission Critical and Mission Essential IT systems.</i></p> <p>The DoD CIO must certify (for MAIS programs) and confirm (for MDAPs) that the program is being developed in accordance with the CCA before Milestone approval. One of the key elements of this certification or confirmation is the DoD CIO's determination that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.</p>
R1196	<p>DoD Instruction 5000.2, Enclosure 4, Table E4.T1 <i>Clinger-Cohen Act (CCA) compliance requires that "[t]he program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards."</i></p>
R1197	<p>DoD Directive 8500.1, Information Assurance (IA) This directive establishes policy and assigns responsibilities under 10 U.S.C. 2224 to achieve Department of Defense information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to net-centric warfare.</p>
R1198	<p>DoD Instruction 8500.2, Information Assurance (IA) Implementation <i>This instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoD Directive 8500.1.</i> [R1197]</p>
R1199	<p>DoD Instruction 8580.1, Information Assurance (IA) in the Defense Acquisition System <i>This instruction implements policy, assigns responsibilities, and prescribes procedures necessary to integrate Information Assurance (IA) into the Defense Acquisition System; describes required and recommended levels of IA activities relative to the acquisition of systems and services; describes the essential elements of an Acquisition IA Strategy, its applicability, and prescribes an Acquisition IA Strategy submission and review process.</i></p>
R1201	<p>DAU Guidebook Section 7.3.4.2. Compliance with Applicable Global Information Grid (GIG) Key Interface Profiles (KIPs), http://akss.dau.mil/dag/Guidebook/IG_c7.3.4.2.asp .</p>
R1204	<p>24 June 2005, <i>Air Force Internet Protocol Version 6 (IPv6) Policy and Transition Plan Tasking</i></p>
R1205	<p>June 2006, <i>DoD IPv6 Transition Plan, Version 2.0</i></p>
R1206	<p>DoD Instruction 8520.2; 1 April 2004; <i>Public Key Infrastructure (PKI) and Public Key (PK) Enabling</i>; http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf</p>
R1217	<p>DoD 8320.02-G, April 12, 2006, <i>Guidance for Implementing Net-Centric Data Sharing</i>; http://www.dtic.mil/whs/directives/corres/pdf/832002g.pdf</p>
R1232	<p>DoD Directive 5230.9, <i>Clearance of DoD Information for Public Release</i>, 09 April 1996</p>

Part 4: Node Guidance

R1291	DoD Instruction 8510.01 , DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007; available at http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf (superseded DoD Instruction 5200.40, DITSCAP)
-------	--