Office of the Assistant Secretary of Defense for
Networks and Information Integration/Department of
Defense Chief Information Officer

Net-Centric Checklist

February 13, 2004

Version 2.1

This Page Intentionally Blank

Foreword

The purpose of the Net-Centric Checklist is to assist program managers in understanding net-centric attributes required for programs to move into the net-centric environment in the Global Information Grid. The Checklist will be updated as needed to reflect DoD standards and industry best business practices. As standards and protocols are approved in the Joint Technical Architecture or the Net-Centric Operations Warfare Reference Model, they will be added to this checklist.

Programs must address the Department of Defense's Net-Centric Data Strategy for:

- Ensuring that data are visible, available, and usable when needed and where needed to accelerate decision-making
- "Tagging" of all data (intelligence, non-intelligence, raw, and processed) with metadata to enable discovery of data by users
- Posting of all data to shared spaces to provide access to all users except when limited by security, policy, or regulations
- Advancing the Department from defining interoperability through point-to-point interfaces to enabling "many-to-many" exchanges typical of a network environment

To implement the Information Assurance (IA) Strategy to transition to a net-centric environment, programs must take advantage of the following:

- An integrated Identity Management, Permissions Management, and Digital Rights Management
- Ensuring that adequate confidentiality, availability, and integrity are provided

The Net-Centric Operations Warfare Reference Model represents the target viewpoint of the Department's Global Information Grid. This viewpoint is a service-oriented, inter-networked, information infrastructure in which users request and receive services that enable operational capabilities across the range of (1) military operations, (2) DoD business operations, and (3) Department-wide enterprise management operations. As programs plan for the future, this NCOW RM must be included in the program planning.

The NII points of contact for this Checklist are Susan E. Shekmar (susan.shekmar@osd.mil) and John Kreger (jkreger@mitre.org).

Table of Contents

Definitions

Global Information Grid: Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

Net-Centricity: Net-centricity is an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, (Net-centricity) translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.[1]

Net-Centric: Exploitation of advancing technology that moves from an application centric[2] to a data-centric[3] paradigm – that is, providing users the ability to access applications and services through Web services – an information environment comprised of interoperable computing and communication components.

Communities of Interest (CoI): Collaboration 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.[4]

Net-centric Information Environment: An information environment that utilizes emerging standards and technologies to optimize assured information sharing among all users. It results from implementing Global Information Grid (GIG) component architectures in accordance with the NCOW RM. A net-centric information environment is inclusive of Core and COI enterprise services, and a data sharing strategy that emphasizes metadata concepts, shared information spaces, and the task, post, process, use (TPPU) paradigm.[5]

[1] Alberts, David S., Garstka, John J., and Stein, Frederick P., *Network Centric Warfare: Developing and Leveraging Information Superiority,* 2nd Edition (Revised), 1999, CCRP Publication Series.

[2] Application-Centric—focusing on the application as the foundation or starting point. In an application-centric system, the program is loaded first, which in turn is used to create or edit a particular type of data structure.

[3] Data-Centric—focusing on the central design data repository as the foundation or starting point. In a data-centric system, the data is primary and services manipulate the data.

[4] DCIO DoD Net-Centric Data Strategy, dated 9 May 2003.

[5] NCOW-RM, 1.0, September 30, 2003

Acronyms

Acronym	Definition
BGP4	Border Gateway Protocol Version 4
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CND	Computer Network Defense
COI	Communities of Interest
CONOPS	Concept of Operations
COOP	Concept of Operations
CRD	Capabilities Requirements Document
CSS	Cascading Style Sheets
DCID	Director of Central Intelligence Directive
DDI	Description, Discovery, and Integration
DDMS	DoD Discovery Metadata Standard
DIACAP	DoD Information Assurance Certification and Accreditation Program
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DoD AF	DoD Architecture Framework
DoDI	Department Of Defense Instruction
FTP	File Transfer Protocol
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IAS	Information Assurance and Security Measures
IC	Intelligence Community
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv6	Internet Protocol Version 6
ISO	International Organization for Standardization
JTA	Joint Technical Architecture
MHTML	MIME HTML
MIME	Multi-purpose Internet Mail Extensions
MOP	Maintenance Operation Protocol
NCOW RM	Net-Centric Operations Warfare Reference Model
NETOPS	Network Operations
OV	Operational Views
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
QoS	Quality-of-Service
REST	Representational State Transfer
RFC	Request For Comment
SAML	Security Assertions Markup Language

SLA	Service Level Agreements
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SV	System Views
TCP	Transport Control Protocol
TV	Technical Views
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USC	Universal Multiple-Octet Coded Character Set
W3C	World Wide Web Consortium
Web-DAV	Web Distributed Authoring and Versioning
WSDL	Web Services Description Language
WS-I	Web Services Interoperability
XML	eXtensible Markup Language
XPath	XML Path Language
XSD	XML Schema Definition
XSL	eXtensible Stylesheet Language
XSLT	eXtensible Style Language Transformations

Net Centricity

The Checklist is divided into four sections:

- Data
- Services
- IA / Security
- Transport

The following questions summarize many of the Checklist questions to focus on the future. As the Department of Defense transitions to the net-centric environment, mission capabilities must support and implement these tenets to meet future operations.

Net-Centric

How is the program Net-Centric? If not, when is it programmed to be? If not programmed to be, what is the sustainment plan?

DoD Joint Technical Architecture

Describe the IT / NSS standards that the program has implemented from the DoD Joint Technical Architecture (DoD JTA, Version 6.0). If not, when is it programmed to do so? If not, explain why they are not being used.

DoD Net Centric Operations and Warfare Reference Model

How is the program aligned with the DoD NCOW Reference Model, Version 1.0? If not, when it programmed to be aligned?

Architecture Views

Be prepared to provide architecture view products (Operational Views [OV], System Views [SV], and Technical Views [TV]) which comply with the product definitions in the DoD Architecture Framework (DoD AF)? If not, when is it programmed to have these products?

The Checklist questions are designed to gather program information to assist DoD leadership in better understanding our move to net-centricity. Questions are tagged as Foundational [F] or Discovery [D]. Foundational questions relate to a net-centric attribute and Discovery questions relate to how programs implement a feature.

Net-Centric Checklist

I. Data

The Net-Centric Data Strategy is a key enabler of the Department's transformation by establishing the foundation for managing the Department's data in a net-centric environment. Key attributes of the Strategy include:

- Ensuring data are visible, accessible, understandable, and trustable when needed and where needed to accelerate decision-making.
- "Tagging" of data (intelligence, non-intelligence, raw, and processed) with metadata to enable discovery by known and unanticipated users in the Enterprise.
- Posting of data to shared spaces for users to access except when limited by security, policy, or regulations.

Data asset refers to any entity that involves data. For example, a database is a data asset that comprises data records.

A. DoD Net-Centric Data Strategy

1. [F] Describe how the program is aligned with the DoD Net-Centric Data Strategy.

   Explain how the program "posts data before processing" (data available on the net as soon as it is created / acquired).

   If not, when is it programmed to be aligned?

   What controls are in place to ensure processes encourage the posting of data for activities to be executed?

B. Design Tenet: Make data visible

1. [F] Does the program provide discovery metadata, in accordance with the DoD Discovery Metadata Standard (DDMS), for all data posted to shared spaces?

   Rationale – Users and applications will migrate from maintaining private data (e.g., data kept within system specific storage) to making data available in community- and Enterprise-shared spaces (e.g., servers and services available on the Internet). Data will migrate from being maintained in private data stores alone, to being made available in community and Enterprise shared spaces.

2. [F] Is all of the data that can and should be shared externally beyond the programmatic bounds of your program visible (i.e., advertised) to all potential consumers of the data?

[F] Describe how the program is making its data assets visible to consumers.

Rationale – Question will identify if the application is making use of Web services to expose its data.

3. [F] Describe how consumers are able to locate the data assets available from your program.

   Rationale – Does a consumer need to know about a data asset and establish a point-to-point connection, or can the data asset be "discovered?"

4. [F] Describe how the program is making use of Web service standards (e.g., SOAP, WSDL, UDDI) to make its data assets visible.

   Rationale: Question will elicit whether the program is taking advantage of some of the open standards for Web services. (Also referenced in Net Centric Operations and Warfare – Reference Model)

5. [D] Describe any subscribe/notify mechanisms for the visible data assets available within the program that alert users and other applications when data has been created or updated.

   Rationale – Question will elicit whether a consumer can be notified when data assets change.

6. [D] Describe where potential consumers can go to become aware of the data assets being made visible by your program.

   Rationale: Question should elicit how the program's data is being advertised to potential consumers.

7. [D] Describe how the program provides dynamic, flexible, and threat-tailorable solutions for exchanging data assets between different security domains (i.e., cross-domain) with flexibility to accommodate new operational needs with minimal impact on system and mission performance.

   Rationale: DoD 8500 series, DCID 6/3

C. Design Tenet: Make data accessible

1. [F] Is all of the data that can and should be shared externally beyond the programmatic bounds of your program accessible to all potential consumers of the data with sufficient access permissions and without any additional programming effort?

   [D] Describe for each visible data asset what the data consumer needs to access the data (e.g., an application client, a Web portal, access to a Web service, access to a shared data storage area, an XML schema/parser, etc.)?

Are there any limitations for the client appliance (e.g., workstation, desktop, laptop, PDA) to access your data assets?

Rationale: Question will elicit whether the program is client neutral and supports standard presentation protocols

2. Has the program explicitly identified the potential universe of consumers of that data? (local, COI, enterprise)

   Rationale – Designers will focus on the immediate requirement for satisfying sponsor demands.

3. [D] Describe the program's architecture and the data separation from the presentation and business logic.

   Rationale – Question will elicit whether the program is an n-tier architecture where the data has been isolated from the business logic.

4. [D] Describe the security mechanisms used to restrict access to specific, visible data assets. Are there any mechanisms in place to protect the data in transit to the consumer?

   Rationale – Question will elicit whether appropriate security has been placed on data assets.

5. [D] Describe how the visible data assets are made available to other users outside the Community of Interest with a need for the data.

   Rationale – Question should help the assessor assess how easily accessible the data.

6. [D] Describe the common design patterns employed in the program that aid in the accessibility of data assets.

   Rationale – Question will elicit whether the program is making use of design patterns to simplify and standardize how data assets are accessed.

7. [D] Describe the use within the program of the following design patterns:

   - Request-Response
   - Publish-Subscribe
   - Transactional or Read-Only
   - Synchronous or Asynchronous
   - Model-View-Controller.

   Rationale – Question will elicit more detailed discussion than the previous question. However, the program will not necessarily employ all of these patterns.

8. [D] Describe how the program provides assurance that there is timely and reliable access to data assets anytime, anywhere for authorized users/entities.

Rationale: DoD 8500 series, DCID 6/3. Integrity is a core IA function, and is necessary to provide confidence in data received

D. Design Tenet: Make data understandable

1. [F] Is all of the data that can and should be shared externally beyond the programmatic bounds of your program sufficiently documented and understandable that any potential consumer can comprehend the structural and semantic meaning to determine how they may use it appropriately?

   [D] Describe how the program tags data with discovery metadata.

   Rationale – Metadata tagging enables users to discover the data for retrieval. The assessor should assess whether sufficient use of metadata is being made.

2. [D] Explain how the program is making use of the DoD Metadata Registry and Clearinghouse.

   Rationale – Question will elicit indicates whether discovery metadata is being generated that is compliant with the DoD Discovery Metadata Specification.

3. [D] Describe the source of all XML elements.

   Has the DoD Metadata Registry been used whenever possible?

   Have newly defined XML elements been registered with the Registry?

   Rationale – Question will elicit whether the program is making use of existing, registered data elements from the Registry.

4. [D] Describe any data schemas or standards being applied in the program.

   Rationale – Question will elicit whether the program is using XML Schemas, DTDs, or something similar to describe its data assets.

5. [D] Describe any automated mechanisms that are available for data mediation/translation (e.g., XSL, XSD).

   Rationale – Question will elicit any data translation capabilities that are available.

E. Design Tenet: Make data trustable

1. [F] Can all potential consumers of all of the data available from your program determine the data pedigree (i.e., derivation and quality), security level, and access control level of your data?

   Rationale: Question will elicit how a consumer can determine data asset quality.

2. [D] Describe for each visible data asset in the program whether the program is the authoritative data source.

   Rationale: Question will elicit whether any data assets are secondary sources.

3. [D] Describe what measures the program takes to ensure the integrity of the data (for internally used data, externally used data, and data that simply transits the program).

F. Design Tenet: Make data interoperable

1. [F] Does all of the data that can and should be shared externally beyond the programmatic bounds of your program have sufficient metadata descriptions and automated support to enable for mediation and translation of the data between interfaces?

   [D] Describe any programmatic changes that would need to be made to the program if a new consumer of a visible data asset were identified.

   Rationale: Question will elicit whether new consumers can be added with no additional cost / effort or whether a new point-to-point interface needs to be established.

2. [D] Identify the published net-centric interoperability standards (e.g., DDMS) to which the program adheres.

G. Design Tenant: Provide Data Management

1. [F] Is there sufficient management of all of the data available through your program to adequately maintain and improve your data assets within a changing environment?

   [D] Describe the effort associated with the program to define, develop, and maintain an ontology (i.e., schemas, thesauruses, vocabularies, key word lists, and taxonomies) that best reflects the community understanding of the “visible data assets”.

2. [D] Describe your processes for ensuring the usefulness and timely availability of all data assets associated with your program.

3. [D] Describe the various data survivability scenarios considered in your program.

   Rationale: Question will elicit the data survivability capability of the program and the consumer’s experience as a result.

H. Design Tenant: Be Responsive to User Needs

1. [F] Are perspectives of users, whether data consumers or data producers, incorporated into data approaches via continual feedback to ensure satisfaction?

2. [D] What tools, services, processes, and resources is the program providing to facilitate user feedback and program responsiveness with respect to data needs?

   Rationale: This question helps determine if the program is putting in place appropriate mechanisms to enable responsiveness to user data and application needs.

3. [D] What metrics are being used to determine responsiveness to user data needs?

   Rationale: This question helps determine the program's ability to measure its responsiveness to user data and application needs.

4. [D] What is the degree of collaboration with respect to data that is enabled and is occurring among the user community(ies) and the program developers?

   Rationale: This question helps assess the actual degree of visibility into ongoing user needs and the responsiveness and quality of interaction with respect to user data and application needs.

5. [D] What are measured / assessed trends over time with respect to the program's responsiveness to user data needs and degree of satisfaction towards meeting those needs?

   Rationale: This question helps determine the degree of program improvement in being responsive to user data and application needs over time.

6. [D] What are the programs plans to enhance responsiveness to user data needs?

   Rationale: This question helps determine potential for improving future responsiveness to user data and applications needs.

II. Services

Services provide an environment that enables the rapid development and deployment of services, with well-defined, realizable capabilities that can be used with other services to provide a range of simple and complex functions

A. Design Tenet: Service-Oriented Architecture

1. [D] Describe how the program will make its unique services/applications available to the GIG community.

B. Design Tenet: Open Architecture

1. [F] Is the architecture based on loosely coupled interactions, enabling the internal components to map to well-defined external interfaces? Describe.
2. [F] Are Web services implemented by the program built using the following core standards?

   a. Web Foundational

   - Hypertext Transfer Protocol (HTTP) Version 1.1, IETF RFC 2616. This is a mandated standard identified in paragraph 3.4.1.8.1 – as of Volume I of the JTA.
   - Hypertext Markup Language (HTML) 4.01, W3C Recommendation. This is a mandated standard identified in paragraph 2.5.4.1 – as of Volume I of the JTA.
   - File Transfer Protocol (FTP), IETF Standard 9, IETF RFC 959. This is a mandated standard identified in paragraph 3.4.1.3 – as of Volume I of the JTA.
   - User Datagram Protocol (UDP), IETF Standard 6, IETF RFC 768. This is a mandated standard identified in paragraph 3.4.1.4.2-as of Volume I of the JTA.
   - Transport Control Protocol (TCP), IETF Standard 7, IETF RFC 793. This is a mandated standard identified in paragraph 3.4.1.10.1-as of Volume I of the JTA.
   - Internet Protocol (IP), IETF Standard 5, IETF RFCs 791, 792, 950, 919, 922, 1112. This is a mandated standard identified in paragraph 3.4.1.11 – as of Volume I of the JTA.
   - Simple Mail Transfer Protocol (SMTP), IETF RFCs 1870, 2821. This is a mandated standard identified in paragraph 3.4.1.1 – as of Volume I of the JTA.

- Multi-purpose Internet Mail Extensions (MIME), IETF RFCs 2045-2049. This is a mandated standard identified in paragraph 3.4.1.1-as of Volume I of the JTA.
- Uniform Resource Locator (URL), Uniform Resource Identifier (URI), IETF RFCs 1738, 1808, 1866. IETF RFC 1738 is mandated in paragraph 3.4.1.8.2 – as of Volume I of the JTA.
- Unicode universal character set, International Organization for Standardization (ISO) 10646, "Universal Multiple-Octet Coded Character Set (UCS)", IETF RFC 2277 http://unicode.org. This is a mandated standard identified in paragraph 2.5.8 – as of Volume I of the JTA.

b. Web Emerging Standards or Best Practices

- HTTP State Management Mechanism, IETF RFC 2965XML Schema 1.0 (http://www.w3.org/TR/xmlschema-1, http://www.w3.org/TR/xmlschema-2). This standard is currently not included in the JTA, but is being considered as a standard to be supported within NCES
- MIME Encapsulation of Aggregate Documents such as HTML (MHTML), IETF RFC 2557 (to aggregate multi-resource documents in MIME-formatted messages). This standard is currently not included in the JTA, but is being considered as a standard to be supported within NCES.
- Web Distributed Authoring and Versioning (Web-DAV), IETF RFCs 2518, 3523. This standard is currently not included in the JTA, but is being considered as a standard to be supported within NCES.

c. XML Foundational

- XML Namespaces (Version 1.0: http://www.w3.org/TR/REC-xml-names, Version 1.1: http//www.w3.org/TR/xml-names11). This is a mandated standard identified in paragraph 2.5.4.1-as of Volume I of the JTA.
- Extensible Style Language Transformations (XSLT) (http://www.w3.org/TR/xslt). This is an emerging standard identified in paragraph 2.5.4.1-as of Volume II of the JTA.
- Extensible Style Language (XSL) (http://www.w3.org/Style/XSL, http://www.w3.org/TR/xsl). This is an emerging standard identified in paragraph 2.5.4.1-as of Volume II of the JTA.

- XML Path Language (XPath) (http://www.w3.org/TR/xpath). This is an emerging standard identified in paragraph 2.5.4.1 – as of Volume II of the JTA.
- Cascading Style Sheets (CSS) (http://www.w3.org/Style/CSS, http://www.w3.org/TR/REC-CSS1, http://www.w3.org/TR/REC-CSS2). This is an emerging standard identified in paragraph 2.5.4.1 – as of Volume II of the JTA.

d. Representational State Transfer (REST) is a style for using HTTP Get commands to invoke Web services. REST describes an architecture style of networked systems (http://www.ebuilt.com/fielding/pubs/dissertation/top.htm). While REST is not a standard, it does prescribe the use of standards:

- Web transfer: HTTP (all resources are accessed with a generic interface, e.g., HTTP GET, POST, PUT, DELETE).
- Named resource references: URL/URN/URI and XLink (XML hyperlinking technology). Every resource on the Web has its own URI.
- Resource Representations: XML, HTML, GIF, JPEG, etc. These are mandated standards identified in section 2 of Volume I of the JTA.
- Resource Types (MIME Types): text/xml, text/html, image/gif, image/jpeg, etc.

e. Simple Object Access Protocol (SOAP) 1.1 (http://www.w3.org/TR/SOAP). This is an emerging standard identified in paragraph 2.5.4.1 – as of Volume II of the JTA.

f. Web Services Description Language (WSDL) 1.1 (http://www.w3.org/2002/ws/desc, http://www.w3.org/TR/wsdl). This is an emerging standard identified in paragraph 2.5.4.1 – as of Volume II of the JTA.

g. Universal Description, Discovery, and Integration (UDDI) 2.0 (http://www.uddi.org, http://www.oasis-open.org/committees/uddi-spec). This is an emerging standard identified in paragraph 2.5.4.1 – as of Volume II of the JTA.

3. [F] Are Web services products compliant with WS-Security (http://www.oasis-open.org/committees/wss) and the Web Services Interoperability (WS-I) Basic Profile V1.0 specification (http://www.ws-i.org/Profiles/Basic/2003-08/BasicProfile-1.0a.htm)?

C. Design Tenet: Scalability

1. [D] What estimates of service usage have been developed (How many expected consumers? How many service invocations per hour (or per some appropriate unit of time)? What assumptions or empirical tests are these estimates based?

2. [D] What performance analysis has been done to understand or predict the ability of the service to handle the expected load (e.g., number of end-user consumers or number of calling services)?

D. *Design Tenet: Availability*

1. [F] Does the program have a continuity of operations plan?

   [F] What is the plan for providing service during routine maintenance (hardware and software)?

   [F] What is the plan for providing service during catastrophic failures (e.g., massive outages of the power grid, physical destruction of the hosting facility)?

   [F] Does the continuity of operations plan include procedures for finding, housing, and supporting the technical support staff during an emergency action?

2. [F] What threat scenarios have been considered and planned for?

E. *Design Tenet: Accommodate heterogeneity*

1. [D] How will the service adapt to delivering capabilities over a range of bandwidths (from low bit-rate tactical communications to multi-gigabit backbone service), and end-user devices (e.g., PDAs, laptops, workstations, mainframes)?

2. [D] Describe how the program will support delivery of capabilities to thin or browser-based clients, especially those that provide adaptability to a variety of disadvantaged ‘edge’ environments for end-users.

F. *Design Tenet: Decentralized operations and management*

1. [D] Does the service offering depend on or use any other services provided by a different program or service provider? If so, explain how this works.

G. *Design Tenet: Enterprise Service Management*

1. [F] Does the service provide instrumentation to enable the service provider to determine the current operational state and performance level of the service?

Rationale – An organizational, procedural and technical construct that fuses Systems and Network Management, Information Assurance, and Information Dissemination Management capabilities to enhance situational awareness and control over the GIG to obtain information superiority leading to decision superiority.

2. [D] Will service management information be made available to consumers of the service as well as the service provider?

3. [D] What protocols and standards are used to collect and disseminate service management information, and in what format will it be made available (e.g., SNMP, XML, CIM – SNMP and XML are identified as mandated standards in Sections 2 and 3 of the JTA, Volume I. CIM is an emerging standard identified in paragraph 2.5.10a of the JTA, Volume II. CIM is also identified as a target standard in the NCOW Reference Model [vers 1.0]).

4. [F] List and provide completed examples of all Service Level Agreements (SLAs) negotiated by this service provider with others (e.g., transport layer programs, other service providers).

Rationale – These questions indicate the level to which the program is integrating into the GIG from and an administrative and management perspective and the type of dependencies the program envisions having on the GIG infrastructure.

III. IA/Security

The Information Assurance (IA) and security measures (IAS) CESs are a framework and family of services that provide a foundation to implement uniform, consistent, and effective IA. The IAS Core Enterprise Services contribute to, but are not sufficient to ensure the security level of each service. They are invoked as needed by service providers and users to satisfy business and policy requirements and reduce cost.

Information Assurance is defined as: 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.

A. DoD Net-Centric Information Assurance Strategy

1. [F] Explain how the program is aligned with the DoD Net-Centric Information Assurance Strategy. If not, when it programmed to be aligned?

B. Design Tenet: Identify Management and Authentication

1. [D] How does the system use identify management for authentication (e.g., biometrics, Common Access Card, or passwords)?

C. Design Tenet: Mediate Security Assertions

1. [F] Does the program mediate security assertions (to pass security related information between systems, processes, and domains)?

   [F] If yes, how does the program mediate security assertions?

   [F] If no, explain.

   Rationale – This would define the method/standards being used to insert security assertions into the requesting message (e.g., Security Assertions Markup Language [SAML]). This would define whether XML gateways/firewalls are used; the use of Public Key Infrastructure (PKI), SAML-in-SOAP; or whether the service application itself is used to implement XML-signature, XML-encryption, etc.

D. Design Tenet: Cross Security Domains Exchange

1. [D] Does the program need to exchange across security domains (e.g., email, structured data sets, unstructured documents, imagery, etc.)?

   [D] If yes, explain.

2. [D] How does the program accomplish the exchange?

[D] Is this mechanism/capability inherent in the program or dependent upon some other program for this capability and if known, which program?

Rationale – Indicate the type of data to be exchanged and its classifications and/or handling caveats. Indicate between which security domains it will be exchanged (one way/both ways) and type of cross-domain solution (e.g., guard) used.

E. Design Tenet: Manage Identity and Privileges

1. [D] How does the program manage identity and privileges?

   Rationale – Indicate whether the product or service will confirm identity of users and processes through PKI certificates. Will the product or service be access-controlled or open to all users?

F. Design Tenet: Encryption and HAIPE

1. [F] Have system requirements for encryption been coordinated with the High Assurance IP Interoperability Specification working group? If no, explain.

G. Design Tenet: Employment of Wireless Technologies

1. [F] Do you (plan to) employ wireless technologies? If yes, which wireless technology and standards will be used?
2. [D] What confidentiality level (public, sensitive, classified) applies to the data being transmitted via wireless technologies?

H. Other

1. [D] Does the system have the ability to define security relevant events and conduct checks of current and past security relevant events?

   [D] Examples of security relevant events include login attempts/failures, entity/user actions, and management actions.

   Rationale: DoD 8500 series, DCID 6/3. Provides situational awareness, traceability, and analytic support to computer forensics, computer network defense (CND), and ESMNETOPS.

2. [F] Does the system provide a secure IA management capability to prevent or minimize the opportunity to attack the GIG?

   [F] Can the system detect and respond appropriately to anomalies/attacks/ disruptions from external threats, internal threats, and natural causes?

Rationale: DoD 8500 series, DCID 6/3. (GIG CRD IV.B.6.c. [3]) MOE 4.3 - Information Assurance, MOP 4.3.2 Information System Protection and Defense DoD 8500 series, DCID 6/3. (GIG CRD IV.B.2.o) MOE 1.1 - End-to-End Services Processing, MOP 1.1.1 – Support all Information Management Tasks, MOP 1.1.2 – Processability.

3. [F] Does the system provide IA mechanisms to protect GIG processes, resources and information from unauthorized modification, disclosure, and destruction such that all system processes are protected and secured at appropriate levels, and visible to all information assurance operations?

   Rationale: DoD 8500 series, DCID 6/3. (GIG CRD IV.B.2.o) MOE 1.1 – End-to-End Services Processing, MOP 1.1.1 – Support all Information Management Tasks, MOP 1.1.2 - Processability.

4. [F] Does the system enforce the GIG digital IA/security policy rules, attributes and standards and manage the CES based upon the overarching GIG digital IA/ Security policy?

   Rationale: DoD 8500 series, DCID 6/3.

5. [F] Does the system utilize a standard labeling scheme and attributes to determine whether entities can exchange and access information?

   Rationale: DoD 8500 series, DCID 6/3, DoD Data Management Strategy.

6. [F] Does the system utilize enterprise services and information to provide a manual or automated integrated picture of the IA/security posture for the GIG enterprise?

   Rationale: DoD 8500 series, DCID 6/3.

7. How does the system provide:

   a. [F]Protection against modification or destruction of information, services, or resources?
   b. [F]Assurance that protection is not disclosed to unauthorized entities, services, or processes?
   c. [F]Assurance that the originator of and action (e.g., information process) and the recipient of a reaction are known (so that neither can deny having processed that action)?
   d. [F]Assurance that there is timely and reliable access to information, services, and resources anytime, anywhere for authorized users/entities?

   Rationale: DoD 8500 series, DCID 6/3. Integrity is a core IA function and is necessary to provide confidence in data received.

8. **Cross Domain IA**

Source: DoD 8500 series, DCID 6/3

a. [F] Does the system provide dynamic, flexible, and threat-tailorable solutions for exchanging information and services between different security domains (i.e., cross-domain) with flexibility to accommodate new operational needs with minimal impact on system and mission performance?

b. [F] Does the system have digital IA / security policy management capabilities that define, enforce, and manage the digital security policy rules, guidelines and standards for securely exchanging data and services across security domains?

c. [F] Does the system provide a capability that enables security domains with different policy constructs to exchange information and be interoperable?

9. [F] Does the system provide the capability to bind strongly the user / entity physical characteristics and attributes to their digital identity?

10. [F] Does the system provide a means for authenticating all GIG entities and for verifying their access credentials are valid and active?

11. [F] Does the system provide the capability to manage access to the GIG information and resources based upon the GIG digital security policy as well as the entity's credentials, privileges, roles, and profile?

12. [F] Does the system provide proactive measures to protect against known and new vulnerabilities to itself and the rest of the GIG?

13. [F] Does the system provide a defensive capability that contains, recovers, restores, and reconstitutes itself or the GIG against incidents (e.g., failure, anomaly, attack, misuse, intrusion, etc)?

14. [F] Does the system have an IA capability to provide timely, reliable access to processes and data even in the event of a denial of service attack?

15. [F] Does the system have an IA capability that provides adequate protection from user attempts to circumvent system access controls, accountability or procedures for the purpose of performing unauthorized system operations?

16. [F] Will the system meet and maintain minimum IA Defense in Depth standards, including certification and accreditation in accordance with Defense Information Technology Security Certification and Accreditation Process (DITSCAP) (or DOD Information Assurance Certification and Accreditation Program [DIACAP]) process (e.g., *CJCSI 6510.01C*, *DoDI 5200.40*)?

17. [F] Does the system have an IA capability to perform content-based encryption of information objects at the host instead of depending on the bulk encryption of the entire network to secure the information and this

capability shall also be available for operations involving allied and coalition forces?

18. [D] Has an information assurance risk management program been developed?

19. [D] Is a Concept of Operations (CONOPS) & COOP program in place (i.e., documentation, training, testing, technical, physical, etc.)?

20. [D] What ongoing intrusion, detection, monitoring, reacting, and auditing capabilities will be implemented in the system?

21. Does the information exchange requirement associated with this system require information exchange across different security enclaves?

22. [D] Does the system have requirements for handling coalition or multi-national data?

23. [D] What security measures handle security at the boundary of the system?

24. [D] What measure does the system take to ensure the integrity of the data (for internally used data, externally used data, and data that simply transits the system)?

25. [D] How will addressable IP devices be protected from denial of service attacks? What criteria do these devices have for availability?

26. [D] What measures are in place to protect against role or identity theft?

IV. Transport

The Transport Infrastructure is a foundation for Net-Centric transformation in DoD and the Intelligence Community (IC). To realize the vision of a Global Information Grid, ASD/NII has called for a dependable, reliable, and ubiquitous network that eliminates stovepipes and responds to the dynamics of the operational scenario – bringing Power to the Edge. To construct the Transport Infrastructure DoD will:

- Follow the Internet Model
- Create the GIG from smaller component building blocks
- Design with interoperability, evolvability, and simplicity in mind

Questions in this category aid in developing an understanding of the general philosophy used in designing the system under assessment. These questions are based on the belief that wherever possible systems should follow the "Internet model" with the goal of becoming "plug and play" building blocks of the Global Information Grid. The design tenet questions test to this ideal, but should not be looked at as qualifying or disqualifying gates.

A. Design Tenet: IPv6

Source: Memo, Internet Protocol Version 6 (IPv6), June 9, 2003, and Memo Internet Protocol Version 6 (IPv6) Interim Transition Guidance, September 29 2003.

1. [F] Describe the program's migration plan to an IPv6 environment. If not, when is it programmed to migrate?
2. [D] What transition technologies such as tunneling, dual stack, etc., are being adopted?
3. [D] Describe the transition approach in terms of network topology (e.g., what regions of the networks are IPv4 and what regions are IPv6).

B. Design Tenet: Packet Switched Infrastructure

1. [F] Describe any information flow between networks within your system or between your system and networks external to your system which is not in the form of IP packets/datagrams.
2. [F] Describe any information flow between networks within your system or to/from networks external to your system that does not pass through an IP router or layer-3 (IP) packet switch.
3. [D] Describe the method(s) by which your system can accept IP datagrams from external networks that are destined for hosts within your system, and the ability of your system to act as a transit network for IP datagrams with an origin and destination that are external to your system.

Rationale – A fundamental assumption of the Internet model is that the infrastructure is best described as "an IP datagram delivery system consisting of a packet switched communications facility in which a number of distinguishable networks (including any networks external to this system) are connected together using routers."

C. Design Tenet: Layering, Modularity

1. [F] Describe all instances in your communications infrastructure where a logical or physical coupling or dependency exists between different layers of the protocol stack (e.g., if your system were to replace Ethernet with Token-Ring at layer 2, would the routing protocol you currently use at layer 3 fail or degrade?

   [F] If you replace a current signal in space with a new physical layer signal does your current layer 2 or layer 3 fail or degrade?).

   Rationale – Probably the only inviolable characteristic of the Internet model is change. Realizing that change will occur and that change occurs at different rates in different elements of the network / protocol stack, GIG systems must be designed to accommodate that change. The most effective way to enable differential change in a system is through modular, layered design.

D. Design Tenet: Transport Goal

Full convergence of traffic (voice, video, data) on a single IP inter network

Source: Memo, End-to-End Information Assurance for the GIG, July 7, 2003.

1. [F] Describe the process (and protocols) used to provide full convergence of traffic (voice, video, and data) on a single IP inter network.
2. [D] What provisions have been made for increased redundancy using resource / path diversities since single link or node failure will take down three (voice, video and data) or more services at the same time?
3. [D] If secure voice is part of the system, is it interoperable with other strategic and tactical secure voice systems with a 99% Threshold Key Performance Parameter? Is the secure voice system interoperable with coalition forces?

E. Design Tenet: Network connectivity

Network Connectivity to all end points such as wide- and local area networks and direct connections to mobile end users

1. [F] What link (layer-2) protocols will be used for transport of IP traffic?

   What standards are being used for these protocols?

[F] Are these standards in the JTA, Version 6.0?

2. [F] What terminal or radio-to-network interfaces will be used for transport of IP traffic?

   What standards are being used for these interfaces?

   Are these standards in the JTA, Version 6.0?

3. [F] What network-to-end user host interfaces will be used for transport of IP traffic?

   [F] What standards are being used for these interfaces?

   [F] Are these standards in the JTA, Version 6.0?

4. [F] Does the system avoid any single point of failure by using multiple connectivity paths (not susceptible to the same threat) and media?

F. Design Tenet: The concurrent transport of information flows

The concurrent transport of information flows from multiple user segments spanning multiple security domains

1. [F] Describe the process (and protocols) that are used to provide convergence of traffic from multiple security domains on a single IP inter-network.

2. [F] Describe the approach for providing an information infrastructure with a colorless or black core.

G. Design Tenet: Differentiated management of Quality-of-Service

Differentiated management of Quality-of-Service (QoS) to ensure required levels of availability by application and function

1. [F] Describe the approach used to provide a priority-based differentiated management of quality-of-service.

2. [D] Describe the approach used to support interoperable management of quality-of-service with external networks.

   Describe any other aspect of the programs QoS support interaction with that of adjacent domains.

3. [D] What measures of quantitative QoS requirements are supportable, for example jitter, latency, throughput, packet loss, others?

4. [D] Describe your program’s alignment with the DoD QoS / CoS working group roadmap.

H. Design Tenet: Inter Network connectivity

Inter Network connectivity to all end points such as wide- and local area networks and direct connections to mobile end users

1. [F] What is used as the inter-domain routing Protocol (e.g., BGP4)? How is it being used? Which system interfaces is it being used on?

2. [F] Describe the autonomous system boundaries. Describe the interface between internal autonomous systems and external autonomous systems which are not under your administrative control.

3. [F] Does the premise router (router that provide the interface between the system being evaluated and external networks) implement features, functions, interfaces, and protocols using open system, non-proprietary methods, if available, that are recognized by appropriate industry standards bodies, working groups, or consortiums?

   [F] What proprietary protocols are required on the premise router?

4. [D] Describe the data interfaces that the premise router supports to external networks.

5. [D] Describe the methods employed to authenticate routing updates on the premise router.

6. [D] Describe the filter/access lists to the control plane including route policy updates from external sources.

7. [D] Describe how the premise router exchanges network reachability information with external networks. What protocols are used?

8. [D] Describe how the premise router authenticates BGP routing information from external networks.

I. Design Tenet: Joint Technical Architecture

Source: Waiting for Ver. 6.0 letter, see also Intro to Ver. 6.0

1. [F] Describe the standards and protocols used that are not in the JTA, Version 6.0.

J. Design Tenet: RF Acquisition

Source: Memo, Radio Frequency (RF) Equipment Acquisition Policy, June 17, 2003.

1. Describe all radio acquisitions that are not JTRS/SCA compliant.

K. Design Tenet: Joint Net Centric Capabilities

Source: Memo, Joint Net Centric Capabilities, July 15, 2003.

1. [F] Describe the standards and protocols that are used to provide connectivity to allied and coalition partners.

2. [D] Describe the type of guard technology used (if used).

3. [D] Describe the standards and protocols that are used to provide connectivity from your network to GIG-BE and TCM.

L. Design Tenet: Operations and Management of Transport and Services

Source: GIG Capabilities Requirements Document (CRD), GIG Network Operations (NETOPS)

1. [F] What are key elements of the management systems architecture (e.g., EMS, Sub-NMS, NMS, associated MIBs, physical and logical connectivity, etc.) in the domains defined by this program?

   [F] How do they interface with one another and with network elements?

   [F] State if these individually and collectively meet GIG-JTA requirements, DoD policies, and use industry standards.

   [F] Specify particular standards used.

   [F] Explain the reasons for required deviation from standards.

2. [F] What management functions exist to comply with requirements on Information Assurance and security?

   How do they interface with other IA systems in the GIG and in legacy networks?

   How are the keys distributed and managed?

3. [D] How will the network management in this program work in joint operations?

   [D] How will they interact with their counterparts in other networks?

   [D] What are the standards used?

4. [D] Does the system have a network management capability to perform automated fault management of the network, to include problem detection, fault correction, fault isolation, and diagnosis, problem tracking until corrective actions are completed, and historical archiving?