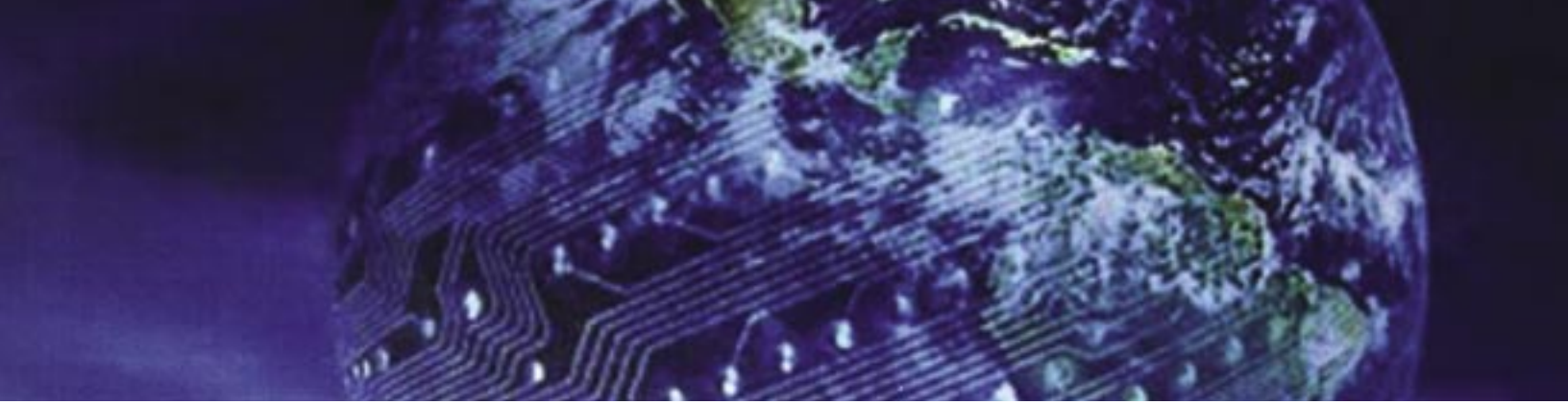


Mission: Possible

SECURELY CONNECTING PEOPLE WITH INFORMATION

John G. Grimes

Defense transformation hinges on the recognition that information is our greatest source of power. Information can be leveraged to allow decision makers at all levels to make decisions faster. Ensuring timely and trusted information is available wherever, whenever, and to those who need it most is at the heart of the capability required to conduct Net-Centric Operations (NCO).

Transforming to NCO requires people, processes, and technology to work together to enable timely:

- Access to information
- Sharing of information
- Collaboration among those involved

Instead of "pushing information out" based on individually engineered and predetermined interfaces, Net-Centricity ensures that authorized users at any level can both "take what they need" and "contribute what they know."

However, the benefits of Net-Centricity unquestionably hinge on one fundamental prerequisite: Information Assurance (IA). The user must have confidence that the information can be trusted to be available and authentic when used.

Yet the threat to our information is real—it is multi-faceted, sophisticated, and increasing daily. Today, firewalls and software patches attempt to keep intruders out and data safe. Tomorrow's assured information will require that the data be secured throughout its lifespan. The IA community must address today's challenges, as well as develop new and innovative capabilities to avert and mitigate tomorrow's threats.

IA is an enabler of one of the most significant military transformations in over 50 years. Significant progress has been made through hard work, innovative thinking, and deep commitment. However, much remains to be done. This document re-affirms the IA Strategy and Architecture, updates relevant policies and plans, and describes accomplishments to date. While the challenge may appear daunting, the outcome is critical. Ultimately, success will be measured in lives saved.

As Chief Information Officer (CIO) and leader of the Department of Defense (DoD) Information Enterprise, I thank you for your commitment and look forward to an exciting journey ahead.

John G. Grimes

Department of Defense (DoD)
Chief Information Officer (CIO)

The Power of
INFORMATION
Access Share Collaborate

We face new challenges in the 21st century

The challenges to national security and global stability will vary greatly. “Uncertainty is the defining characteristic of today’s security environment” (Quadrennial Defense Review). The challenges will involve asymmetric operations, a wide range of partners, compressed timelines, worldwide visibility, and non-state enemies who seek to destroy our free way of life. Success in this new strategic environment requires levels of responsiveness and agility never before demanded of our Armed Forces. We must confront uncertainty with agility. One of the keys to becoming more agile is the ability to access and leverage trusted and timely information as needed, rather than based on predetermined distribution schemes with extended analysis delays. As the Department of Defense (DoD) continues its transformation from an Industrial Age mindset to a 21st Century force, information is at the heart of NCO.

For true Net-Centricity to be achieved information has to be more than just available—it must be trusted. Assured information allows decisions to be made with speed, accuracy, and confidence. When the integrity of information is compromised the results can be devastating—national security and lives are at stake.

The Information Assurance (IA) community has been implementing a strategy to:

- Protect information
- Defend systems and networks
- Provide situational awareness and command and control
- Transform and enable IA capabilities
- Create an empowered workforce

In the Net-Centric world,
trusted information
is the key

the key

Table of Contents

Vision of a Net-Centric Environment 2
DoD's IA Strategic Plan. 6
Full Spectrum GIG Operations 9
IA Component of the GIG Integrated Architecture. 10
IA Implementation Guidance. 12
Daily Execution 14
It Starts with You. 16

A Vision of a Net-Centric Environment

National Security Strategy

"Transforming America's national security institutions to meet the challenges and opportunities of the Twenty-first Century."

National Defense Strategy

"We will conduct Net-Centric Operations with compatible information and communications systems, usable data, and flexible operational constructs.

"Beyond battlefield applications, a network-centric force can increase efficiency and effectiveness across defense operations, intelligence functions, and business processes.

"Transforming to a Net-Centric force requires fundamental changes in process, policy, and culture."

National Military Strategy

"Creation of a collaborative information environment that facilitates information sharing, effective synergistic planning, and execution of simultaneous, overlapping operations...on demand to defense policy-makers, warfighters and support personnel."

We must create a secure Net-Centric Environment

The top defense leaders in this country have all outlined a vision of a Net-Centric Environment (NCE) that moves information where and when it is needed, to those who need it most.

Operating in this new kind of environment requires our Armed Forces to achieve higher levels of responsiveness and agility. These tough demands come at a time of increased surprise and uncertainty, adding to the challenge while making them a higher priority.

DoD CIO Vision

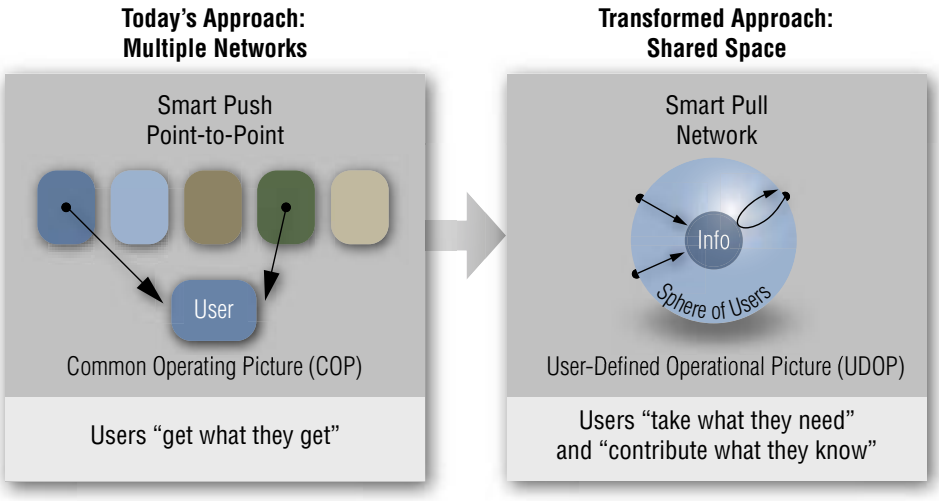
Deliver the Power of Information

An agile enterprise empowered by access to and sharing of timely and trusted information.

DoD CIO Mission

Enable Net-Centric Operations

Lead the Information Age transformation that enhances DoD's efficiency and effectiveness.



Net-Centricity requires IA

Imagine a Net-Centric world where a unit in the field can access information, such as which building an insurgent entered, as soon as it is available and posted without delays for analysis and action.

Accessible information gives troops the ultimate advantage on the battlefield, but it is critical that warfighters can depend on the information they are given. If the adversary intercepts or compromises information, missions fail and lives may be lost.

Defense networks face new attacks every day, including worms and viruses, network flooding, infrastructure assaults, insider threats, and data theft.

We must stay steps ahead of those who would weaken our information networks and systems. In order to achieve the Net-Centric Vision, our priority must be to secure the networks using IA.

Strong IA enables:

Trust—Commanders can trust and rely on the integrity of the information and networks they use to make decisions. If the commander doubts the information or if it has been compromised, the advantages of speed and agility are lost.

Timeliness—The GIG means 24/7 availability of information on-demand. More importantly, it means getting the information when it is needed without delay.

Accessibility—Net-Centric Operations have removed the limitations of time and geography. Strong IA enhances and enables interoperability and reduces stovepipes. Additionally, interoperability promotes success with multinational and coalition operations and ensures security is an integrated component.

IA Vision

Dynamic IA for the Global Information Grid (GIG)

IA Mission

Assure the Department's information, information systems and information infrastructure and support the department's transformation to network and data-centric operations and warfare

"Achieving the full potential of Net-Centricity requires viewing information as an enterprise asset to be shared and as a weapon system to be protected."

—Quadrennial Defense Review

the GIG

With strong IA, Commanders are confident in their information because five crucial conditions have been met:

1. **Confidentiality**—Information is protected from unauthorized entities or processes
2. **Integrity**—Information is protected from unauthorized modification or destruction
3. **Availability**—Information is timely with reliable access for authorized users
4. **Authentication**—Measures are in place to verify the legitimacy of information and those claiming to be authorized users
5. **Non-repudiation**—Information can be proven to have originated from the sender of record

Excellent IA practices lead to efficiency. With strong IA in place, staffing and materials requirements are decreased. This results in faster response times, reduced hazards to warfighters, and increased combat effectiveness. Strong IA can save lives.

The secured GIG holds the future of warfighting

Net-Centricity will be achieved through the GIG. From its beginnings as a series of loosely connected, unrelated networks, the GIG is evolving into a seamless information environment that provides access to warfighting, intelligence, and business-related processes in ways that are assured, available, and appropriately managed. It is a trusted environment.

Warfighters, other authorized users, and weapons systems can access the GIG at any time, from anywhere in the world, to obtain the information they need to successfully execute their mission. It reduces stovepipes and enables user to access a system of shared information.

As the GIG evolves and matures, DoD will:

- **Build**—Make information available through a network that users know they can trust
- **Populate**—Add new dynamic sources of information to use in defeating adversaries
- **Operate**—Maintain systems and keep the networks fully functional at all times
- **Protect**—Implement new and better ways to eliminate weaknesses

Trusted Information on the GIG

where it is needed | when it is needed | to those who need it most

The GIG balances the often opposing needs of access and security. The GIG's dynamic architecture will allow warfighters and coalition partners access while denying access to the adversary. To be truly effective, integrity and trust must be built into the system at the time of design and not "bolted-on" later.

A comprehensive vision for Net-Centricity and IA means more than just building a secure GIG. It means changing processes and policies. It requires a trained workforce that understands and practices "good IA" and is vigilant at all times. It includes ongoing innovation at all levels of the Department. With all of those elements in place, we are securely connecting people with information—the heart of Net-Centric Operations.

the plan

The IA Strategic Plan lays the foundation for securing the GIG

Securing the GIG involves five major components: DoD's IA Strategic Plan; full spectrum GIG operations; IA component of the GIG Integrated Architecture; and implementation guidance. These actions will secure the GIG and instill user confidence in the information that moves within it.

1

DoD's IA Strategic Plan

Released in January 2004, the first component is a comprehensive Strategic Plan that defines the Department's goals and objectives for IA, and provides a consistent, Department-wide approach for securing the GIG.

Goal 1: Protect information—Safeguarding data as it is being created, used, modified, stored, moved, and destroyed whether at the client, within the enclave, at the enclave boundary, or within the computing environment, to ensure that all information's level of trust corresponds with mission needs.

Goal 2: Defend systems and networks—Recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies to ensure that no access is uncontrolled and all systems and networks are capable of self-defense.

Goal 3: Provide integrated situational awareness/IA Command and Control (C2)—Integrating an IA posture into an operational picture synchronized with NetOps and emerging Joint C2 Common Operating Picture (COP) programs to provide decision-makers and network operators at all command levels with the tools to conduct IA/Computer Network Defense (CND) operations and Net-Centric Warfare.

Goal 4: Transform and enable IA capabilities—Discovering emerging technologies, experimenting, and refining development, delivery, and deployment processes to improve life cycle time, reduce risk exposure, and increase return on investments.

Goal 5: Create an IA empowered workforce—Establish an IA professional workforce with the knowledge, skills, and abilities to effectively prevent, deter, and respond to threats against DoD information, information systems, and information infrastructures and create the capability to place people with the right skills, in the right place, at the right time.

Accomplishments

DoD has realized several significant accomplishments across each of the five goals including:

- Launched the Cryptographic Modernization Program
- Implemented DoD Public Key Infrastructure (PKI) to provide higher trust in identities and improve protection of sensitive data
- Established a DoD Computer Network Defense (CND) Enterprise Solutions Steering Group to acquire, field, and sustain enterprise CND tools
- Implemented automated, enterprise-wide vulnerability management capability to perform automated cyber vulnerability scanning and automated patching
- Created substantial improvements in attack, sensing, and warning capabilities through an enhanced constellation of intrusion and anomaly detection sensors
- Established successful international partnerships increasing critical CND information sharing for enhanced IA/CND programs
- Established a Department-wide standard for IA workforce management and baseline IA knowledge and skills that all personnel performing IA functions must achieve
- Facilitated development of a system administration network attack simulation trainer
- Established DoD/IC Unified Cross Domain Management Office (CDMO)
- Increased Systems Accreditation rate while increasing number of systems reported in IT Registry
- Trained the majority of DoD personnel in computer security awareness despite larger numbers of Service members deployed to combat theaters
- Expanded the number of universities that are Centers of Academic Excellence in IA Education to over 75
- Institutionalized DoD IA Scholarship Program (IASP) to attract and retain top talent and to target academic research to support the mission critical IA/IT needs of the Department
- Expanded Red and Blue Team evaluation activities across DoD to enhance mission readiness
- IA is a regular part of major DoD exercises
- Aligned over 83% of DoD Components to an accredited CND Service Provider
- Issued the IA Component of the GIG Integrated Architecture Version 1.1, providing a GIG IA vision aligned to the GIG IA Initial Capabilities Document

"The IA Team is making a difference"

—Priscilla Guthrie, Principal Deputy DoD CIO

Operationalizing the Plan

The goals in DoD's IA Strategic Plan are enduring and serve to define a consistent strategic direction to assuring information. DoD's IA Strategic Plan is a living document and as such will be continually updated to ensure it remains a vital and accurate reflection of the major issues facing the Department.

The objectives in the Plan are currently being revised to reflect the strategic priorities of the Department defined in the Quadrennial Defense Review. Additionally, it will address the Deputy Secretary of Defense's emphasis on measuring performance based on outcomes to convey how well the Department is performing in response to shoring up today's defenses and preparing for the future.

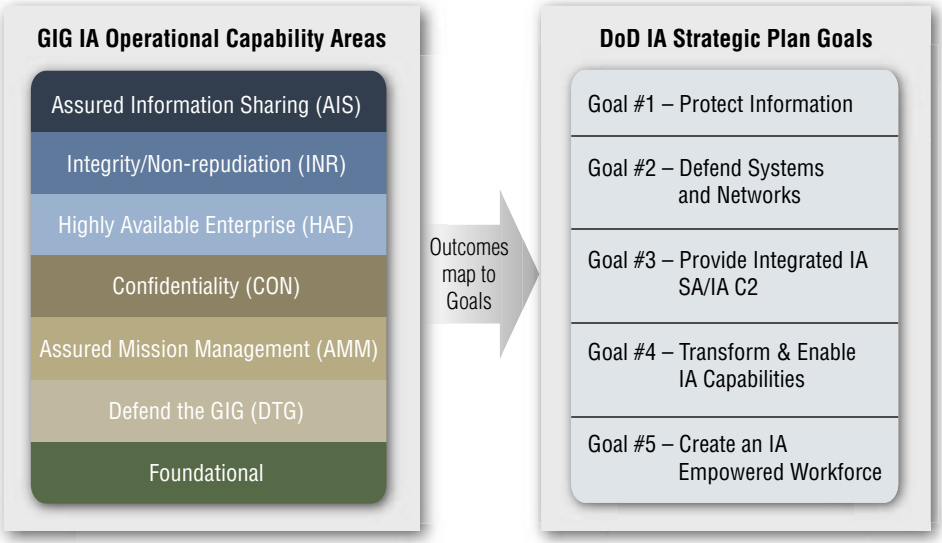
Portfolio Management

The CIO established the GIG IA Portfolio (GIAP) Management Office, to oversee the IA Capability Portfolio and maximize the IA investments enterprise-wide. We are developing an Integrated Performance Management Plan to measure how well we are managing the programs and initiatives in DoD's IA Capability Portfolio and our progress against DoD's IA Strategic Plan.

The IA Capability Portfolio is organized by the IA Operational Capability Areas in the IA Component of the GIG Integrated Architecture. The enabling program and initiative investments in DoD's IA Capability Portfolio are being implemented in order to accomplish the goals and outcome objectives in DoD's IA Strategic Plan.

"Increase investment to implement the GIG, defend and protect information and networks and focus research and development on its protection."

—Quadrennial Defense Review



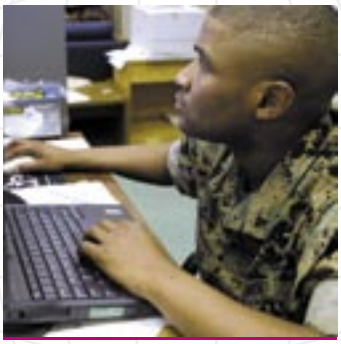
2 Full Spectrum GIG Operations

The second component of the plan strengthens security and enhances the GIG and includes the evolving components of full spectrum GIG Operations. The evolving National Military Strategy for Operations in Cyberspace (NMS-OC) is a comprehensive military strategy for DoD to assure U.S. Military strategic superiority in cyberspace. To ensure coordinated full spectrum of operations across the GIG, Commander, U.S. Strategic Command has designated Joint Task Force-Global Network Operations (JTF-GNO) with GIG operational authority. The JTF-GNO Strategic Plan outlines four strategic areas:

1. **Operations**—Full capability to respond to or direct the operations and defense of the GIG
2. **Technology**—Realize full situational awareness of the GIG through common processes, standards, and instrumentation, enabling near real time manipulation of any asset in order to optimize Net-Centric services
3. **Resources**—Full capability to project, define, advocate and defend JTF-GNO resource requirements to include budget, personnel, training, and certification
4. **Doctrine**—Full capability to establish and maintain relevant, current, and operationally sound NetOps doctrine across DoD, and establish similar guidance for all federal partners

These areas assure the U.S. Military's strategic superiority of cyberspace, and further our standing of defense-in-depth, which supports a robust GIG. Defense-in-depth integrates diverse tactical and operational methods to safeguard networks and platforms.

Earlier versions of defense-in-depth were based on securing the perimeter and adding increasing rings of perimeter security to provide added protection for selected important systems and capabilities. However, as security of the GIG evolves and newer tools become available, we are evolving the defense-in-depth strategy to allow for coordinated full spectrum GIG operations. Technology is being leveraged, and this is transforming the process from a perimeter defense concept, to embedding security across the fabric of the enterprise down to and including the data element. This transformational shift of security, embedded in the fabric, strengthens the security posture and truly adds depth and breadth to our security and operational posture.

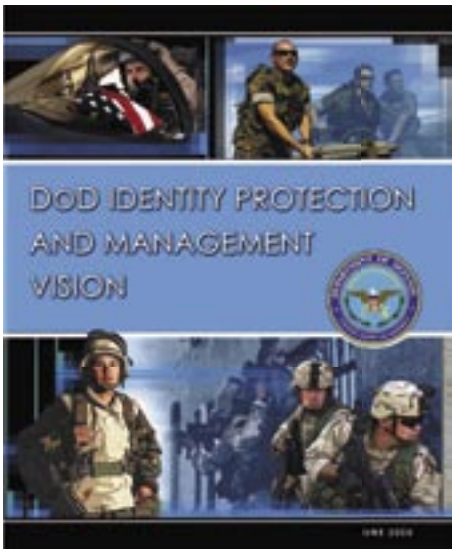


3 IA Component of the GIG Integrated Architecture

A third component of the plan relates to developing standardized architectural concepts for securing and enabling a GIG that has IA built into its basic framework. The IA component of the GIG Integrated Architecture aligns with the GIG IA capabilities defined in the approved GIG IA Initial Capabilities Document (ICD) and the initial Capabilities-Based Assessment (CBA). These capabilities were the foundational basis for the development of IA operational activities, IA system functions, and the incremental capabilities in the IA Transition Strategy.

The GIG Integrated Architecture addresses the security challenges of a NCE that is highly dynamic, highly interconnected and interdependent, and supports users and systems with varying levels of trust.

Transactional information protection—Supporting collaboration and information sharing within the NCE, in which users have varying levels of trust and their systems have varying levels of IA capabilities and trust, requires a dynamic, transactional approach to IA. This permits information exchange to occur only when it is authorized and when the information can be sufficiently protected by the systems that support the information exchange.

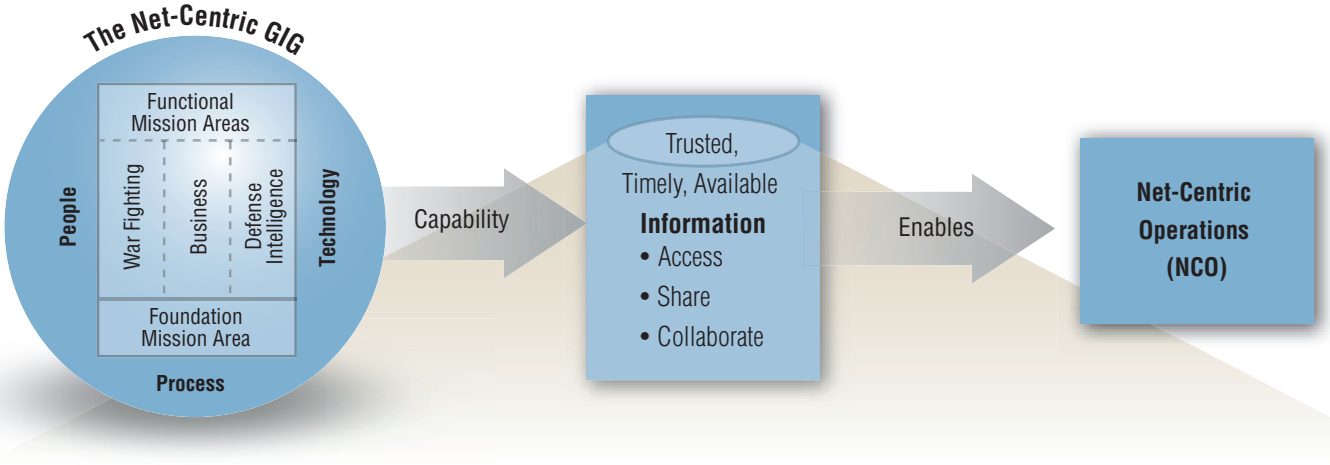


Digital-policy-based enterprise—Increased interdependence and interconnection of Net-Centric systems will challenge our ability to contain attacks and may increase attack avenues available to our adversaries. An enterprise enabled by digital policy allows resources to be adjusted to ensure that the highest-priority missions continue to receive the support needed for success: the dynamic, highly automated, coordinated establishment and enforcement of information access, communities of interest (COI), mission priorities, resource allocations, and responses to cyber attack.

Defense against an adversary from within—The NCE will be constantly threatened from a variety of adversaries, including sophisticated Nation states. Defending against an increased cyber and insider threat as a result of broader information sharing and greater interconnectivity of systems requires an enhanced ability to monitor, track, search, and respond to attacks. These capabilities also enhance our ability to prevent adversaries from gaining insider access and, should they do so, improves the ability of our systems to detect their presence.

Integrated security management—Current Security Management Infrastructure (SMI) practices focus on generating and distributing public key certificates and cryptographic keys. To adequately protect the NCE, which is constantly changing in response to changing mission needs, attacks, and outages, SMI must evolve to support a more automated,

Achieving Net-Centricity: Terms and Relationships



IA Component of the GIG Integrated Architecture

Baseline
- Independent system-high environments
- Multiple coalition and bi-lateral environments per COCOM

Increment 1 Focus
- Hardened, US/Allied integrated Secret environment
- Improved Cross-Domain Solutions (CDS)
- Technology available to other environments including piloting of a Multi-REL warfighting environment

Increment 2 Focus
- High robustness access control; improved misuse detection
- Multi-REL Warfighter COCOM environments
- Integrated Multi-level US/Allied environment

Increment 3 Focus
- High robustness access control; improved misuse detection
- Integrated U—TS/SCI Multi-level, Multi-REL environment

Net-Centric key-management capability that also includes IA enterprise capabilities. Automating these procedures wherever possible will reduce the operational burden and configuration errors, improve real-time support, and minimize dependence on users and system administrators to understand and enforce cyber security.

Enhanced integrity and trust of Net-Centric systems—Operating in a variable trust NCE requires IA functionality to be distributed across the IT components that make up the Net-Centric systems. Achieving the level of integration, flexibility, and cost effectiveness needed to realize the Net-Centric vision requires greater use of commercially available products and greater reliance on software-based IA functionality. Attaining a sufficient level of trust in the IA functionality provided by these hardware and software components is fundamental to achieving an assured GIG.

GIG IA Operational Capabilities are highly interdependent and require that IA deployments be synchronized with the evolution in deployed mission-operational capabilities. DoD must embrace the Enterprise IA transformation if budgets, programs, and policies are to be synchronized for the successful execution of missions at an acceptable level of risk.

IA Implementation Guidance

4

The fourth component of the Department's plan to enhance IA for the GIG is to develop and implement a suite of DoD IA policies that create the conditions for success. The GIG paradigm of the future will present new challenges. In recognition of these challenges, DoD has already begun to devise the strategic requirements and implemented the guidance to fully realize a NCE. These policies and their implementation guidance must accommodate the dynamic nature of the GIG as it transitions from an enclave-oriented to a service-oriented architecture while maintaining appropriate levels of confidentiality, integrity, and availability. Some of the policies and implementation guidance that move us in that direction are as follows:

DoDD 8100.2—Establishes policy and assigns responsibilities for the use of commercial wireless devices, services and technologies in DoD's Global Information Grid. Directs the development and use of a Knowledge Management process to promote the sharing of wireless capabilities, vulnerabilities, and vulnerability mitigation strategies throughout DoD.

DoDD 8115.01—Establishes policy and assigns responsibilities for the management of DoD information technology (IT) investments as portfolios that focus on improving DoD capabilities and mission outcomes. Each program portfolio is managed using the GIG Integrated Architecture, plans, risk management techniques, capability goals and objectives, and performance measures. While this directive does not directly address IA, the portfolio management structure influences the way in which IA programs are managed.

DoDD 8500.1—Specifies the high-level policies and responsibilities that will allow DoD to achieve and maintain appropriate levels of confidentiality, integrity, and availability for all DoD information systems.

DoDI 8500.2—Establishes a multi-tiered management structure to accommodate evolution of the GIG and provides sets of baseline IA controls that must be consistently applied.

DoDI 8510—This soon to be published instruction will establish a standard process for identifying, implementing, and validating IA controls as well as authorizing system operation and managing the IA posture across all of DoD as we transition to the GIG. This Defense Information Assurance Certification and Accreditation Process (DIACAP) instruction will replace the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

DoDI 8520.2—Prescribes procedures and assigns responsibilities for implementing DoD Public Key Infrastructure (PKI) and Public Key Enabling (PKE) to achieve a higher level of confidentiality through cryptography, digital signature, and multiple authentication mechanisms.

DoDD 8530.1 and DoDI 8530.2—These two issuances identify policy, assign responsibilities, and provide procedures essential to support the Commander, USSTRATCOM's CND initiatives. Both policies are currently under revision.

DoD 8530.1-M—Defines a standard process for certifying and accrediting CND Service Providers within DoD.

DoDI 8551.1—Addresses ports, protocols, and services management at the enterprise level to enhance interoperability and security management of ports and protocols in use.

DoDI 8552—This soon to be published instruction will require that mobile code used in DoD undergo a risk assessment, be assigned to a risk category, and have its use regulated based on its potential to cause harm.

DoDI 8570.1—Establishes IA Training, Certification, and Workforce Management requirements and procedures for the entire DoD IA workforce. It also mandates the identification, tagging, and tracking of IA personnel, positions, and certification status.

DoD 8570.1-M—Provides guidance and procedures for the training, certification, and management of DoD workforce conducting IA functions in assigned duty positions and provides information and guidance on reporting IA training metrics.

DoDI 8580.1—Provides for integration of IA into the Defense Acquisition System by specifying required and recommended levels of IA and prescribing an IA strategy process for the acquisition of mission critical and mission essential systems.

DoDD 8581.1—Establishes IA policy and assigns IA responsibilities for all DoD space systems.

CJCSI 6510.01D—Contains detailed procedures for IA and CND that complement the guidance issued in DoD 8500 series directives and instructions.

CJCSI 6212.01C—Includes Net Ready Key Performance Parameters (NR-KPP) and IA requirements for Joint Capabilities and Integration Development System (JCIDS) interoperability and supportability certification and validation of Information Technology and National Security Systems.

In addition to the above mentioned directives and instructions, there are a number of other targeted subject and focus areas in which policy and instructions have been issued or are nearing completion.

Daily Execution

5

The fifth and final component to the Plan is daily execution and implementation. Creating and maintaining a secured network requires the dedication and commitment of everyone. The proper functioning of the GIG is as critical as any other weapon system. Just as operators of specialized weapons systems must be licensed, certified, and held to pre-determined standards, so too must GIG operators be required to undergo training and certification.

In this sense, IA is similar to operational security—everyone has a role, and all must come to the realization that their participation is vital.

- Resource allocators must be made aware of the importance and necessity for IA
- IA professionals within our Armed Services must be trained, certified, and tracked through subsequent duty assignments
- Systems administrators must receive standardized training and certification in the performance of IA functions and understand the need for preparing readiness reports on the systems they administer
- The user community must be educated and certified to ensure necessary levels of competency
- Commanders and staff at all levels must understand the nature of the cyberspace domain of warfare and practice good IA at all times

Just as operators of weapons systems for land, air, or sea must be trained and certified, so too must operators of the weapon system for cyber space—the GIG.


PMUX

your role

Mission: Possible

The GIG is the future of secured information for our Armed Services. When fully deployed and mature, it will serve as the Net-Centric source of trusted on-demand data and intelligence required by our Joint, Allied, and Coalition Forces to achieve full-spectrum dominance. A strong and deliberate IA strategy, governance, and implementation plan that includes personal vigilance on the part of us all is needed to secure the GIG and ensure that sensitive information is both trusted and secure.

It Starts with You

A secured GIG can only be achieved with the dedication and commitment of everyone. To be effective, Commanders must establish the climate, commit resources, organize and train personnel, and accept responsibility for protecting the GIG.

Protection of the GIG requires a strong and deliberate IA strategy, governance, and implementation plan supplemented with personal vigilance.

Operationalizing Information Assurance

To learn more about Information Assurance and how it can support your specific mission, please contact:

DoD Chief Information Officer
6000 Defense Pentagon
Washington, DC 20301-6000
http://www.dod.mil/nii