Secure From the Start: Designing and Implementing an Assured National Security Enterprise

LTG Keith B. Alexander
National Security Agency/Central Security Service

The Global Information Grid (GIG) information assurance (IA) architecture is the embodiment of an Enterprise IA model and is being designed to support the entire National Security Enterprise with input from the Department of Defense, Department of Homeland Security, and intelligence community. It is an essential enabler of the GIG Net-Centric Warfare vision. National Security Agency (NSA) architects have identified innovative IA approaches to support dynamic, secure enterprise-wide information sharing. Portfolio management for the effort is being provided by the GIG IA Portfolio Management Office at NSA in partnership with Office of the Secretary of Defense, and the Military Services, commands and agencies.

The Global Information Grid (GIG) is a Department of Defense (DoD) initiative to develop an assured global information technology (IT) enterprise that will enable its strategic objectives of information superiority and net-centric warfare (NCW). NCW is a set of warfighting concepts and capabilities that provide for worldwide access to information and services – anytime, anyplace – allowing the warfighter to take full advantage of all available information and bring all available assets to bear on the mission in a rapid and flexible manner. To achieve this vision, the DoD is transforming the way it operates, communicates, and uses information to include expanding user access to a much richer set of information and collaboration capabilities. Information assurance (IA) is a critical enabler of the GIG and the DoD strategic objectives.

Roles and Responsibilities

The National Security Agency/Central Security Service (NSA/CSS) is an active participant, partner, and leader in making net-centricity a reality. Due to NSA/CSS's unique position of performing both offensive and defensive missions, the Assistant Secretary of Defense for National Information Infrastructure (ASD/NII) tasked NSA/CSS to provide the IA architectural guidance and IA portfolio management to deliver the DoD's GIG vision. We are partnering with U.S. Strategic Command (STRATCOM), the Joint Staff, the Defense Information Systems Agency (DISA), and the Military Services in defining and implementing a secure, net-centric operating environment. Additionally, we are working with the intelligence community (IC) to drive the increased sharing of critical data securely.

The NSA/CSS's Enterprise IA Architecture and Systems Engineering Office, in partnership with the GIG community, leads the effort to define a GIG IA architecture that includes enterprise-level IA strategies, guidance, standards, policies, systems requirements, and technologies necessary to realize DoD's net-centric GIG vision. While the office's principal focus is on supporting the GIG, its work is broadly applicable to net-centric enterprise efforts across the IC, Department of Homeland Security (DHS), Information Sharing Environment (ISE), and other federal information technology (IT) enterprises. These national security communities require the development of an assured global national security IT enterprise to transform the way they operate, communicate and use information to accomplish their missions. NSA/CSS's IA support will help ensure that communications, information sharing, and infrastructure availability are not barriers to the nation's security.

> *"Dynamic interactions in a net-centric collaboration and information-sharing environment require a greater level of interdependency between systems."*

IA Vision

The DoD net-centric IA vision is to enable a dynamic, information-sharing environment that delivers secure information at the right time, to the right recipient, and in the right format under every circumstance. This environment must be securely managed and protected enterprise-wide from threats posed by adversaries. Providing enterprise-wide protection of the dynamic information-sharing environment requires a cohesive, integrated approach to IA that enhances policies, procedures, technologies, and training.

Enterprise IA Model

In the past, a system-high security approach was taken to secure the system containing the information. The system-high security model requires the system to operate at the level of the highest information classification and the protection mechanisms be approved to protect the highest classification level of information contained within the system. Additionally, every user had to be cleared for that level of access (i.e., if the highest classification of information being processed in a system is SECRET, then all the systems and interconnections involved in sharing this information need to be protected and need to meet the security requirements for protecting SECRET information).

Dynamic interactions in a net-centric collaboration and information-sharing environment require a greater level of interdependency between systems. The traditional system-high security approach cannot be used to support dynamic interactions between systems in this variable environment. The dynamic interactions occur in an environment where trustworthiness

varies between the users participating in the collaboration and sharing, the systems supporting the collaboration and sharing, and the sensitivity levels of the information being shared. These collaborative users form groups commonly referred to as communities of interest (COI). A COI is any group of users that needs to exchange information to accomplish a given mission. COIs may be pre-established users with ongoing agreements, or may develop on an ad-hoc basis and may include both traditional (e.g., coalition forces for military engagements) or non-traditional partners (e.g., federal, state, or local government agencies in support of disaster relief missions). The dynamic interactions require that the protection approach for information sharing shift to a transaction-based *Enterprise IA model*.

Under this new model, information exchanged as part of a transaction is protected to a level appropriate for the information being exchanged. That is, dynamic mechanisms are used to determine whether or not information should be shared and under what conditions. The approach to realizing the assured GIG vision is shaped by the following set of guiding principles essential for the transformation of IA:

- **Separation of Information Protection from Infrastructure Protection** (i.e., protecting information wherever it resides). Past IA models focused predominantly on protecting the physical computing and data storage devices and their communications infrastructure (e.g. gates, guards, dogs, and link/network encryptors). Net-centric IA will augment and evolve current communication infrastructure protections to allow for a dynamic, distributed perimeter where end-to-end object-level information protection reduces (and perhaps eventually replaces) the physically separate networks used across the community today. This includes protecting data in storage, packets, messages, and sessions in transit in addition to the networks.
- **Policy-Driven Enterprise.** The impacts of system outages, degradations, and cyber attacks will significantly expand in the net-centric environment. Interdependence and interconnection of systems will affect our ability to contain these impacts. A digital policy driven enterprise that enables dynamic, highly automated and coordinated establishment and enforcement of information access, mission priority, resource allocation, and cyber attack response will counter this increased threat. It will also provide the ability to adjust resources to ensure that the highest priority missions receive the resources needed for their success.
- **Support for Varying Levels of Trust.** Today we define a single standard for protection of information that resides within a system-high environment. As we move forward into the highly interconnected net-centric environment, the enterprise will need to ensure information is sufficiently protected while supporting collaboration and information sharing across environments where the users and their systems have varying levels of trustworthiness.

"We must develop and apply robust tools, technology, and operational approaches to actively defend our networks."

- **Persistent Monitoring and Misuse Detection.** Counterbalancing the increased cyber and insider threats brought about by the broader sharing and greater interconnectivity of systems requires enhanced cybersituational awareness and network defense capabilities. We must develop and apply robust tools, technology, and operational approaches to actively defend our networks. A key part of this strategy is to shift to a distributed enterprise sensor grid, in which IT components throughout the enterprise provide sensor inputs. Persistent monitoring develops cybersituational awareness through analysis of the sensor grid inputs across classification levels, missions, and COIs. This capability is critical to improving the ability to detect misuse and insider threats.
- **Greater Use of IA-enabled IT Components.** Today's IA capabilities are implemented in a bolt-on approach (e.g. add-on security products) as specialized IA appliances primarily deployed at the enterprise perimeters. The Enterprise IA model requires IA functionality to be distributed across IT components as well as greater reliance on software-based IA functionality combined with greater assurance and trust in the host computing platforms. This new enterprise protection model *bakes in* IA functionality by requiring it to be designed and built into IT components from their inception, and requires increased trustworthiness in those components to correctly perform their IA functionality. The terms *bolt on* and *baked in* are diametrically opposed. Bolted-on security implies that it has been added after the fact. Baked-in security requires that the security features be designed and integrated throughout the system lifecycle, from concept. *Baked in* is inherently superior because it guarantees that complementary, mutually supportive approaches and technologies are employed.
- **Evolution to Dynamic Security Management.** Today, the management of security is primarily focused on the generation and distribution of public key certificates and cryptographic keys for cryptographic devices. In an environment where enterprise protection relies on an array of IA-enabled IT products, the concept of security management must expand to support not only a more automated, net-centric key management capability, but it must also evolve to support security services such as identity, privilege, audit, and IA configuration management. With the development of a more comprehensive toolkit of security management capabilities, they can be applied to support the active defense of our networks by dynamically reconfiguring access to network resources as directed by network security policy and informed by persistent monitoring and situational awareness.

GIG IA Architecture

The GIG IA architecture is the embodiment of the *Enterprise IA model* into a set of architectural products (e.g., operational, system, and technical views) that defines the IA strategies and capabilities to ensure protection

of the information, availability, and assured control of the GIG IT infrastructure. Assured operation in the high-risk, end-state environment of the GIG will require unprecedented changes to its information, services, and infrastructure. Full integration of IA solutions, with the appropriate IA functionality and robustness within nearly every IT component of the GIG enterprise, will be paced by resources and commitment. Thus, over the next decade, the GIG enterprise will undergo an incremental evolution toward the end-state vision with new IA capabilities phased in as operations, technologies, resources, and policy permits. The gap between the near-term capabilities and the end-state vision will be bridged through one or more incremental rollouts of interim IA capabilities. The GIG IA architecture strategy will serve as the foundation for delivering IA capabilities to the IC, DoD, NSA/CSS, DHS, ISE, and other federal agencies comprising the National Security Community.

GIG IA Portfolio Management: Implementing the GIG IA Architecture

On October 10, 2005, the Deputy Secretary of Defense approved the DoD IT Portfolio Management Directive, otherwise referred to as DoD Directive 8115.01. This directive dramatically changes the way that DoD manages major initiatives and the projects that comprise them. To comply with the guidance referenced in the introduction, the DoD Chief Information Officer (CIO), as the Enterprise Information Environment Mission Area (EIEMA) lead, established Enterprise Information Environment domains, and named domain owners, including the Office of the Assistant Secretary of Defense/Networks and Information Integration as the domain owner for IA. The latter, in turn, appointed the Director, National Security Agency (DIRNSA) as the IA domain agent to lead the DoD's portfolio management IA activities. In September 2005, DIRNSA created the GIG Information Assurance Portfolio (GIAP) management office to execute these duties on his behalf. Though located at NSA/CSS and initially staffed with NSA/CSS personnel, this is a community office and will eventually grow to include other community members from across the national security community.

Developing an assured GIAP will not be *managing* all of the service and agency IA programs. That will be left to the services and agencies themselves. The GIAP has established a community-wide portfolio management working group to work closely with ASD/NII and its defense-wide IA program office, and representatives from STRATCOM, Joint Staff, DISA, and the Services to examine the IA programs to determine the capabilities they deliver and the capabilities they are depending on to achieve success as well as at the timing of the programs to ensure they are aligned. This synchronization is important to ensure that DoD dollars are being invested optimally.

"The GIG is an exciting and challenging undertaking that will need participation and partnership by the DoD, IC, DHS, industry, and academic communities."

The GIG is an exciting and challenging undertaking that will need participation and partnership by the DoD, IC, DHS, industry, and academic communities. NSA/CSS has defined a *defense-in-depth* IA strategy that relies on intrinsic, baked-in security and dynamic management, which focuses on protecting information in addition to the communications networks. That, along with extrinsic testing and analysis of residual risks and implemented with sound network security design, provides effective 24/7 operations.

NSA/CSS continues to contribute to the information sharing needs of the men and women serving in harms way, actively fighting terrorism, and defending our country. NSA/CSS has committed senior-level managers, technical leaders, and a deep cadre of technical experts to make the GIG vision, through the GIG IA architecture and portfolio management, a success.◆

Information Sources

1. Department of Defense Directives: <www.dtic.mil/whs/directives>.
2. Department of Defense Global Information Grid: <www.defenselink.mil/nii/global_Info_grid.html>.
3. Department of Defense Global Information Grid Information Assurance: <https://gesportal.dod.mil/sites/gigia>.

About the Author

LTG Keith B. Alexander, USA, is the Director, National Security Agency/Chief, Central Security Service (NSA/CSS), Fort George G. Meade, Md. As the Director of NSA and Chief of CSS, Alexander is responsible for a combat support agency of the Department of Defense with military and civilian personnel stationed worldwide. He entered active duty at the U.S. Military Academy at West Point. Among previous assignments, Alexander has served as Deputy Chief of Staff (DCS, G-2), Headquarters, Department of the Army, Washington, D.C.; Commanding General of the U.S. Army Intelligence and Security Command at Fort Belvoir, Va; Director of Intelligence, U.S. Central Command, MacDill Air Force Base, Fl; and Deputy Director for Requirements, Capabilities, Assessments and Doctrine, J-2, for the Joint Chiefs of Staff. He holds a Bachelor degree from the U.S. Military Academy, a Master of Science degree in Business Administration from Boston University, a Master of Science degree in Systems Technology (Electronic Warfare) and a Master of Science degree in Physics from the Naval Postgraduate School, and a Master of Science degree in National Security Strategy from the National Defense University.

National Security Agency
9800 Savage RD
FT George G. Meade, MD 20755
Phone: (301) 688-6524
E-mail: nsapao@nsa.gov