Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2008	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
An Introduction to the Deputy Assistant Secretary of Defense for Information and Identity Assurance	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Deputy Assistant Secretary of Defense for Information and Identity Assurance 6000 Defense Pentagon RM 3E240 Washington, DC 20301-6000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
CROSSTALK The Journal of Defense Software Engineering July 2008

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**3**	

An Introduction to the Deputy Assistant Secretary of Defense for Information and Identity Assurance

Robert Lentz
Deputy Assistant Secretary of Defense for Information and Identity Assurance

Trusted information, anytime, anywhere is the vision of the year-old Office of the Deputy Assistant Secretary of Defense for Information and Identity Assurance (DASD[IIA]). Every functional, operational, domain, and institutional-based joint capability of the Department of Defense (DoD) is information dependent and relies on trusted information to function effectively. The DoD faces daily attacks on its networks and systems, ranging from curious kids to much more advanced, organized campaigns. The DASD(IIA) team is providing a defense-in-breadth approach to protect our systems, networks, and information.

Defense transformation hinges on the recognition that information is a key strategic resource within the DoD and across government agencies. This information is a critical component of situational awareness, allowing decision makers at all levels to quickly turn information into decisions and, ultimately, into actions. Ensuring timely and trusted information is available wherever, whenever, and to those who need it most is at the heart of net-centricity. Net-centricity ensures that authorized users at any level can take what they need and contribute what they know.

The benefits of net-centricity unquestionably rely on one fundamental prerequisite: identity assurance. Users must have confidence that information has integrity – it has not been tampered with; authenticity – it is from a trusted source; and availability – it will be accessible when needed, even in the face of attack. Threats to our information are real, multi-faceted, sophisticated, and growing in number and effectiveness. Additionally, the DoD's missions are increasingly dependent on the information technology (IT) underpinnings provided by the Global Information Grid (GIG). The GIG's resiliency and continuity of mission-essential functions is a priority as sophisticated adversaries improve knowledge of our capabilities. Moreover, as the business and operational environments in which we operate continue to change almost daily, we can neither predict when nor how today's technologies will be overtaken by more advanced technologies, nor can we predict how events around the world will affect future requirements and what the costs will be to protect our assets. The Information Assurance (IA) community's challenge is to address today's challenges while developing new and innovative capabilities to avert and mitigate tomorrow's threats and the impact of yet-unknown external factors.

Recognizing the importance of a secure, trusted network, the Honorable John J. Grimes, Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD[NII]/DoD CIO), recently created the Office of the DASD(IIA). The office was created from the IA Directorate; formally part of the deputy CIO's office, and elevated the oversight of IA throughout the DoD from a director-level position to the level of a deputy assistant secretary.

... as the business and operational environments in which we operate continue to change almost daily, we can neither predict when nor how today s technologies will be overtaken by more advanced technologies ...

The new office is organized around the following directorates:

- The IA Policy and Strategy Directorate, responsible for providing IA policy and strategic direction to enable capabilities required to deliver IA throughout the DoD. To include devising and advancing IA strategic initiatives, enabling assured net-centric operations, developing domestic and coalition cyber partnerships, and influencing secure and resilient network architectures.
- The Defense-wide IA Program (DIAP) Directorate, responsible for ensuring the DoD's vital information resources are secured and protected through IA compliance by applying a defense-in-breadth methodology that integrates the capabilities of people, operations, and technology to establish multilayer, multi-dimensional protection.
- The Identity Assurance/Public Key Infrastructure Directorate, responsible for providing DoD-level direction and guidance for enterprise-wide identity services that ensure the availability of an operational identity management infrastructure consistent with the architectural constructs established in the GIG.
- The Globalization Task Force, responsible for developing and overseeing implementation of a strategy for mitigating national security risks arising from the increasing globalization of the information and communications technologies infrastructure consistent with the objectives of ASD(NII)/DoD CIO and national policy.
- The Defense Industrial Base Cyber Security Task Force, responsible for securing critical DoD programs and technology by protecting DoD controlled unclassified information resident on defense industrial base networks through the development, implementation, and execution of DoD policy, resources, structure,

and processes in collaboration with DoD components, industry, and other federal government departments, collectively known as the interagency.
- A DoD senior IA engineer and chief technology officer to provide advice on IA engineering programs and projects and emerging technical challenges, planning and execution of the GIG IA Portfolio Management Office (GIAP) and enterprise-wide systems engineering efforts.

In addition to the these directorates, the office is tasked with management oversight for the GIAP and tasked with analyzing, selecting, controlling, and evaluating critical IA capabilities and associated investments to enable information superiority to deliver the best mix of IA capabilities, ensuring cyberspace dominance across the full range of military operations. The Unified Cross Domain Management Office is tasked with providing centralized direction, coordination, and oversight for all cross domain activities and investments within the DoD.

IA within the DoD previously relied on a *defense-in-depth* approach to assuring information based largely upon firewalls and software patches; the focus was on attempting to keep intruders out and data safe. As approaches to IA have evolved, the DoD is moving towards a *defense-in-breadth* approach, integrating capabilities of people, operations, and technology to establish a multi-layer, multi-dimensional protection that will assure our information warfare capabilities and information-critical components are trusted throughout their lifespan to achieve decision/mission superiority.

This defense-in-breadth approach will be highlighted in a rewrite of the DoD IA Strategic Plan (SP) to be completed this year. The original DoD IA SP provided a shared vision, goals, objectives, and a consistent, enterprise-wide approach for securing the GIG since its release in January 2004. As stated in the first version of the DoD IA SP, it is a living document and we are committed to updating it to keep it vital and to accurately reflect the major IA issues confronting the DoD. As such, an updated version of the DoD IA SP was signed by the ASD(NII)/DoD CIO in March 2008[1]. The revised plan reaffirms the vision and goals introduced in 2004 for assuring information and updates relevant objectives and the actions critical to securing the net-centric GIG and achieving our long-term vision: delivering the power of information: access – share – collaborate. The following five goals introduced in 2004 remain in the 2008 interim version and continue to be the cornerstone of the DoD IA SP:

- **Goal 1: Protect information to achieve assured information sharing.** Achieving this goal of trusted data anywhere on the Net requires partnerships and combined efforts with other components of the security community (i.e., physical security, personnel security, and critical infrastructure protection) in order to provide an integrated systems security posture.
- **Goal 2: Defend systems and networks.** The points of focus for this goal are the Computer Network Defense protection, detection, and reaction mechanisms for DoD systems and networks and adaptive configuration management, a critical capability that includes both active and passive defenses necessary to correctly respond to legitimate but changing demands while simultaneously defending against adversary-induced threats.
- **Goal 3: Align GIG mission assurance through integrated IA situational awareness and IA command and control.** The complex and interdependent nature of our information networks and the demands of net-centric warfare require shared awareness and understanding across the enterprise to enable effective command and control. Combatant commanders require sufficient visibility into their network operations, including the threats to these networks and the IA capabilities applied to protect, defend, and respond to them.
- **Goal 4: Transform and enable IA capabilities.** Transforming IA capabilities depends heavily on the ability to influence the processes the DoD uses to create, assess, test, and implement new ideas. Developing new approaches to problem solving depends on the synergy between each process as an idea progresses from concept to reality. The focus of this goal is to influence the development of three key processes (acquisition, planning, and innovation) to further the IA mission and support the transformation of the force.
- **Goal 5: Create an IA-empowered workforce.** This goal addresses IA awareness, technical training, and security management. IA awareness is targeted to all DoD employees, from entry-level to senior executive service to flag officer. Technical training and education focuses on system and network administrators and personnel performing maintenance functions on DoD workstations, systems, and networks as well as IA officers, IA managers, designated approving authorities, and their IA staffs.

The planned revision to the Strategic Plan will place significant emphasis on operationalizing full life-cycle security, or defense-in-breadth, and will reflect the strategic priorities of the DoD ...

The planned revision to the SP will place significant emphasis on operationalizing full life-cycle security, or defense-in-breadth, and will reflect the strategic priorities of the DoD outlined in the Quadrennial Defense Review and the CIO's SP. Additionally, it will call out IA as the bedrock underpinning the GIG and place more emphasis on achieving mission assurance by expanding the scope of our third goal: to leverage all elements of information warfare and operationalizing the defense-in-breadth approach.

The DoD has realized several significant accomplishments across each of the five goals to effectively increase its security posture; however, while tremendous progress has been made in validating requirements, defining an architectural road map, operationalizing policies and transformative processes, and developing and deploying innovative technical solutions to the warfighters and business communities, our future success will require a continued focus on the operational aspects of IA, fusing people, processes, and technolo-

gies to combat current and future threats in real-world operational environments. This includes a fusion with the IC.

A significant accomplishment of the new DASD has been the publication of DoD IA Certification and Accreditation Process (DIACAP)[2], which replaces the interim DIACAP instruction released in July 2006. The DIACAP instruction articulates policy and establishes the process for conducting IA certification and accreditation (C&A) of DoD information systems. Replacing the DoD IT security certification and accreditation process, the DIACAP supports the evolution to a net-centric GIG through a dynamic IA C&A process that provides visibility and control of IA capabilities and services, including core enterprise services and Web-enabled systems and applications.

Under the DIACAP, all DoD-owned information systems and DoD controlled information systems operated by a contractor or other entity on behalf of the DoD will be certified and accredited through a standardized enterprise process for identifying, implementing, and managing IA capabilities and services. Through this enterprise process, the DIACAP supports the transition of DoD information systems to GIG standards and a net-centric environment while enabling assured information sharing.

CrossTalk has been gracious enough to devote this issue to DoD IA issues. We hope you find them informative, thought-provoking, and helpful towards understanding the roles, missions, and challenges that face the DoD today and in the future.◆

Notes

1. Available online at the DoD IA Portal, Common Access Card required <https://www.us.army.mil/suite/portal/index.jsp>.
2. DoD Instruction 8510.01. 28 Nov. 2007 <www.dtic.mil/whs/directives/corres/pdf/851001p.pdf>.

Acronym Key for This Issue

AIS: Assured Information Sharing
C&A: Certification and Accreditation
CIO: Chief Information Officer
CNSS: Committee on National Security Systems
DASD(IIA): Deputy Assistant Secretary of Defense for Information and Identity Assurance
DIACAP: DoD Information Assurance Certification and Accreditation Process
DIAP: Defense Information Assurance Program
DISA: Defense Information Systems Agency
DNI: Director of National Intelligence
DoD: Department of Defense
GIAP: GIG IA Portfolio (Management)
GIG: Global Information Grid
IA: Information Assurance
IC: Intelligence Community
INFOSEC: Information Security
IT: Information Technology
NII: Networks and Information Integration
NSA: National Security Agency
NSS: National Security Strategy
R&D: Research and Development
SME: Subject Matter Expert
UCDMO: Unified Cross Domain Management Office
USG: United States Government

About the Author

Robert Lentz is the DASD(IIA) in the OASD (NII)/CIO. He is the chief IA officer for the DoD and oversees the DIAP, which plans, monitors, coordinates, and integrates IA activities across the DoD. Lentz is the Chairman of the National Space INFOSEC Steering Council, a member of the Presidential Subcommittee on National Security Systems, the manager of the DoD IA Steering Council, and the IA domain owner of the GIG Enterprise Information Management mission area. He also reports to the Deputy Undersecretary for Security and Counterintelligence, and is a member of the Information Operations Steering Council. Lentz represents the DoD on several private sector boards, including the Center for Internet Security Strategic Advisory Council, the Common Vulnerabilities and Exposures Senior Advisory Council, and the Federal Electronic Commerce Coalition. He has more than 26 years of experience with the NSA in the areas of financial management and technical program management. He has served as Chief of the Space and Networks IA Office, Chief Financial Officer of the NSA IA Directorate, Executive Assistant to the NSA Signals Intelligence Collections and Operations Group and Field Chief of the Finksburg National Public Key Infrastructure/Key Management Infrastructure Operations Center. In 2004, Lentz received the highest-level honorary award the DoD can bestow on a civilian employee, the prestigious Secretary of Defense Distinguished Civilian Service Award. He holds a bachelor's degree with a double major in history and political science from Saint Mary's College of Maryland, and a master's degree in national security strategy from the National War College.

6000 Defense Pentagon
RM 3E240
Washington, DC 20301-6000
Phone: (703) 695-8705
E-mail: robert.lentz@osd.mil