Securing the Global Information Grid – The Way Ahead for Information Assurance

Richard Aldrich
Booz Allen Hamilton

David Zaharchek
IBM

The Department of Defense's (DoD) Information Assurance (IA) Strategic Plan provides a solid foundation and framework for securing the information, and the DoD has realized several significant accomplishments across each of five goals to effectively increase the DoD's security posture of the DoD. Our future success will require a continued focus on the operational aspects of IA to combat current and future threats in real-world operational environments. The threats facing the DoD are real. Our networks are under attack daily and our adversaries are growing ever more sophisticated. To effectively defend its systems and networks, the DoD is implementing a multi-layered, defense-in-depth approach.

A 2006 report released by the General Accountability Office (GAO), titled *Suggested Areas for Oversight for the 110th Congress* [1], provided recommendations for 36 oversight areas for the incoming 110th Congress. One recommendation included in the GAO report suggested the DoD develop and implement viable strategic plans with goals, objectives, key milestones, and measures to monitor and report on progress in transforming its key business operations. The DoD IA community has outpaced the GAO's recommendation by several years and has set the standard for strategic planning within the DoD. The DoD IA Strategic Plan, released in January 2004, provides a solid foundation and framework for securing the DoD's information, defines the DoD's goals and objectives for IA, and provides a consistent, department-wide approach for securing the Global Information Grid (GIG). The DoD IA Strategic Plan has been instrumental in defining the value proposition and building a convincing business case for IA – resulting in more than 54 percent real growth in the DoD's IA budget since 1999.

The cornerstones of the IA Strategic Plan are its five goals:

- **Goal 1: Protect information.** Safeguarding data to ensure that the level of trust for all information corresponds with mission needs.
- **Goal 2: Defend systems and networks.** Recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies.
- **Goal 3: Provide integrated IA/ Network Operations (NetOps).** Providing 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, improving process life-cycle time, reducing risk exposure, and increasing return on investment.
- **Goal 5: Create an IA empowered workforce.** Establishing an IA professional workforce with the right skills, in the right place, at the right time.

These goals are enduring and serve to define a consistent strategic direction to keep information secure and trusted while at the same time accessible. The DoD has realized several significant accomplishments across each of the five goals to effectively increase the security posture of the DoD; however, while the DoD has made tremendous progress in defining requirements, developing policies and processes, and developing and deploying innovative technical solutions to the warfighters, our future success will require a continued focus on the operational aspects of IA – fusing people, processes, and technologies – to combat current and future threats in real-world operational environments.

Efforts are under way to ensure personnel have the knowledge and skills to effectively and securely operate and defend the DoD's information systems and networks. The DoD IA Scholarship Program is a highly competitive initiative that provides full scholarships to students who attend National Security Agency-designated centers of academic excellence in IA education in exchange for DoD service. Scholarships are used to recruit new personnel into the DoD and to provide opportunities for current employees to earn advanced degrees in IA related disciplines.

A second, and much broader, initiative is the IA Workforce Improvement Program. Its focus is managing and professionalizing the IA workforce. To do this, the program leverages commercial information technology security certifications, such as those offered by International Information Systems Security Certification Consortium, Information Systems Audit and Control Association, System Administrator, Audit, Network, Security Consortium, Computing Technology Industry Association, and Security Certified Program, to establish a DoD baseline of IA workforce knowledge and skills. All personnel performing IA functions – military, civilian, and contractor – are expected to meet the requirement, whether they do the work as a primary duty or as an additional or embedded duty. Currently, components are in the process of identifying and documenting their IA workforce and preparing them to be certified to the DoD-wide baseline.

The DoD is a robust, worldwide organization that leverages its capabilities through information systems and networks. The increasing reliance upon these information systems and networks for our nation's defense makes their protection critically important. As the DoD becomes more net-centric, it becomes more vulnerable to shared risks where the vulnerabilities of one part of the network could adversely impact many others.

The threats facing the DoD are real. Our networks are under attack daily and our adversaries are growing ever more sophisticated. The DoD's information infrastructure, the GIG, globally pervasive and comprised of millions of hosts and thousands of networks, is subject to hundreds of thousands of attacks, scans, and other incidents every year. To effectively defend its systems and networks, the DoD is implementing a multi-layered, defense-in-depth approach. Some of these enterprise defense-in-depth initiatives include the following:

- The fielding of two commercial tool suites, one to scan for vulnerabilities (Secure Configuration Compliance Validation Initiative) and one to remediate them (Secure Configuration Remediation Initiative). The tools can also check for compliance with best security practices as specified in the DoD's security technical implementation guides and take remedial actions as appropriate. Using these tools, the system administrators can rapidly identify and patch vulnerabilities.

- Increased protection measures on each computer and server. The DoD will soon deploy an enterprise-wide host-based security system capability that will field an integrated package of host-based security applications to help fight today's dynamic network threats. These include the intrusion detection system, host-based intrusion prevention system, host-based firewall, file integrity monitoring and alerting, execution control, self-enforcing configuration control, and information condition management capability. As the DoD increasingly encrypts its communications to the end user, bolstering defenses at the host level is becoming critical.
- Two initiatives supporting insider threat mitigation. One effort is directed broadly at detecting the threat and the second is focused on monitoring those who are suspected insiders. Contracts for this enterprise capability should be awarded in the near term.
- Attribution capability to identify the originators of cyber attacks. This capability is key to the appropriate NetOps response. As such, the DoD has initiated a bolstered forensics effort that will facilitate detailed analysis of systems that were attacked. In addition, the DoD is also developing a *honeygrid* capability as a means of identifying, distracting, and diverting attackers.
- Hardening of the DoD's IT infrastructure with additional firewalls and demilitarized zones (DMZs). The DMZ approach provides a separate interface to the Internet and external DoD connections, thus limiting non-classified Internet Protocol Router Network vulnerabilities to malicious attacks, worms, and viruses that plague the Internet. The DMZ also mediates and regulates external access to DoD applications, data, and public information services pages.

Deployment and distribution of enterprise security tools have been accomplished by various means. These include direct download of the software licenses from the DoD server to the individual user/system administrator as well as direct installation of tools by the DoD or integration contract resources to implement the tools within a local site. Tools designated for general use throughout the enterprise are normally operated by the system administrators at each of the component enclaves. However, a centralized help desk, supporting most of the enterprise capabilities, has been established within the Defense Information Systems Agency to provide information and assistance for tool installation and operation for all DoD users.

Components receive updates to enterprise tools as well as new capabilities through either the normal component budgeting process and/or in combination with the DoD enterprise solutions steering group. This steering group provisions general CND tools enterprise-wide based on identified requirements and funding constraints.

The DoD recognizes securing this vast network of networks requires more than technological solutions. To synchronize these efforts, the DoD developed an IA component of the GIG architecture that defines required capabilities to secure the GIG. These have been further defined as the IA capability areas and are managed as an IA capability portfolio. Portfolio management has been fully embraced by the DoD and provides a framework for analyzing IA investments. The GIG IA Portfolio Management Office manages the IA Capability Portfolio by looking at the many initiatives being funded by elements across the DoD in a disciplined and unified manner, aligning these investments against the GIG IA architecture and the IA Strategic Plan and projecting anticipatory research to address critical challenges in securing the GIG.

The threat environment is constantly changing and evolving, unconstrained by state and national borders. To overcome these challenges, the DoD is diligently working to improve and harden its defenses while expanding cooperation with national and international partners. The IA strategic plan lays the foundation for securing the GIG. However, our future success requires the dedication, commitment, and personal vigilance on the part of all GIG users. In addition to our efforts to secure the GIG through the deployment of new capabilities and the establishment of policies, we must establish a climate of security consciousness, commit resources, organize and train personnel, and accept responsibility for protecting the GIG to achieve mission success. Securing the GIG is the responsibility of us all.◆

Reference

1. "Suggested Areas for Oversight for the 110th Congress." Washington: GAO, 2006 <www.gao.gov/new.items/d07325r.pdf>.

About the Authors

Richard Aldrich is the senior computer network operations policy analyst for the Information Assurance Technology Analysis Center and an associate for Booz Allen Hamilton. He has multiple publications in information security and has presented at several national and international conferences. He has a bachelor's degree in computer science from the U.S. Air Force Academy, a Juris Doctor from the University of California Los Angeles, and a Master of Laws in Intellectual Property Law from the University of Houston.

Booz Allen Hamilton
1215 S Clark ST
STE 1101
Arlington, VA 22202-4302
Phone: (703) 602-9991
Fax: (703) 602-7209
E-mail: richard.aldrich.ctr@osd.mil

David Zaharchek is a managing consultant in IBM Business Consulting Services' Public Sector Business Strategy Practice and has supported strategic planning and performance measurement efforts for the DoD Defense-Wide Information Assurance Program for more than five years. Zaharchek has both public and private sector experience in the areas of corporate strategic planning, strategic resource allocation, and performance measurement and management.

IBM Business Consulting Services
1215 S Clark ST
STE 1101
Arlington, VA 22202-4302
Phone: (703) 653-7028
Fax: (703) 602-7209
E-mail: david.zaharchek@us.ibm.com