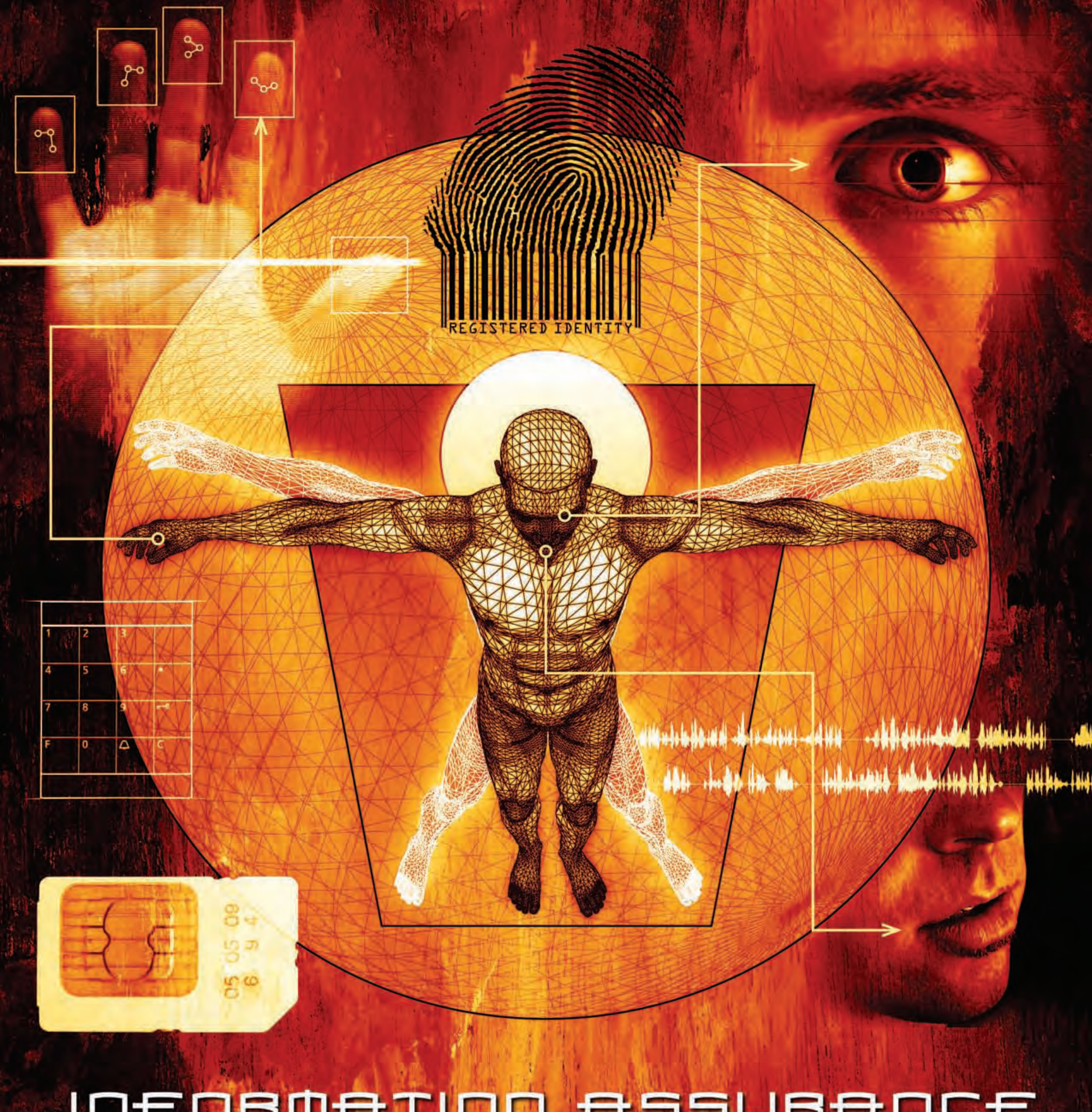
CrossTalk

July 2008 **The Journal of Defense Software Engineering** Vol. 21 No. 7



Information Assurance

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **JUL 2008**	2. REPORT TYPE	3. DATES COVERED **00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE **CrossTalk: The Journal of Defense Software Engineering. Volume 21, Number 7, July 2008**	5a. CONTRACT NUMBER 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) **OO-ALC/MASE,6022 Fir Ave,Hill AFB,UT,84056-5820**	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

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**	**Same as Report (SAR)**	**32**	

Information Assurance

ON THE COVER

Cover Design by
Kent Bingham

Additional art services provided by Janna Jensen

Departments

Updated figures for "Welcoming Software Into the Industrial Fold," by James M. Sutton, published in the May issue, are now available online at <www.stsc.hill.af.mil/crosstalk>.

CROSSTALK

CO-SPONSORS:	
DoD-CIO	*The Honorable John Grimes*
OSD (AT&L)	*Kristen Baldwin*
NAVAIR	*Jeff Schwalb*
76 SMXG	*Phil Perkins*
309 SMXG	*Karl Rogers*
DHS	*Joe Jarzombek*
STAFF:	
MANAGING DIRECTOR	*Brent Baxter*
PUBLISHER	*Kasey Thompson*
MANAGING EDITOR	*Ken Davies*
ASSOCIATE EDITOR	*Chelene Fortier-Lozancich*
ARTICLE COORDINATOR	*Nicole Kentta*
PHONE	(801) 775-5555
E-MAIL	stsc.customerservice@hill.af.mil
CROSSTALK ONLINE	www.stsc.hill.af.mil/crosstalk

CROSSTALK, The Journal of Defense Software Engineering is co-sponsored by the Department of Defense Chief Information Office (DoD-CIO); the Office of the Secretary of Defense (OSD) Acquisition, Technology and Logistics (AT&L); U.S. Navy (USN); U.S. Air Force (USAF); and the U.S. Department of Homeland Security (DHS). DoD-CIO co-sponsor: Assistant Secretary of Defense (Networks and Information Integration). OSD (AT&L) co-sponsor: Software Engineering and System Assurance. USN co-sponsor: Naval Air Systems Command. USAF co-sponsors: Oklahoma City-Air Logistics Center (ALC) 76 Software Maintenance Group (SMXG); and Ogden-ALC 309 SMXG. DHS co-sponsor: National Cyber Security Division of the Office of Infrastructure Protection.

The USAF Software Technology Support Center (STSC) is the publisher of CROSSTALK, providing both editorial oversight and technical review of the journal. CROSSTALK's mission is to encourage the engineering development of software to improve the reliability, sustainability, and responsiveness of our warfighting capability.

S T S C

Subscriptions: Send correspondence concerning subscriptions and changes of address to the following address. You may e-mail us or use the form on p. 19.

517 SMXS/MXDEA
6022 Fir AVE
BLDG 1238
Hill AFB, UT 84056-5820

Article Submissions: We welcome articles of interest to the defense software community. Articles must be approved by the CROSSTALK editorial board prior to publication. Please follow the Author Guidelines, available at <www.stsc.hill.af.mil/crosstalk/xtlkguid.pdf>. CROSSTALK does not pay for submissions. Articles published in CROSSTALK remain the property of the authors and may be submitted to other publications.

Reprints: Permission to reprint or post articles must be requested from the author or the copyright holder and coordinated with CROSSTALK.

Trademarks and Endorsements: This Department of Defense (DoD) journal is an authorized publication for members of the DoD. Contents of CROSSTALK are not necessarily the official views of, or endorsed by, the U.S. government, the DoD, the co-sponsors, or the STSC. All product names referenced in this issue are trademarks of their companies.

CrossTalk Online Services: See <www.stsc.hill.af.mil/crosstalk>, call (801) 777-0857 or e-mail <stsc.webmaster@hill.af.mil>.

Back Issues Available: Please phone or e-mail us to see if back issues are available free of charge.

Confronting Cyber Uncertainty

We live in a truly global society shaped by the advent of the telephone, the data network, the jet airliner, and, now, the Internet. As the impact of globalization spreads, all of us – in business, government, and our private lives – have come to depend on the Internet. Its influence cannot be overstated. The Internet is pervasive, accessible to a growing number of people, and it enables us to do things we would have thought impossible not long ago. I wish I could say all this was good, but like so many technologies, there are downsides. Information can be stolen, damaged, and denied on the Internet. Personal identities, intellectual capital, even valuable military data, can be compromised and manipulated. Criminals, terrorists, and nations can – and do – exploit the vulnerabilities in computers and networks for their own purposes. In spite of all the growth and advancement we have seen, the global strategic environment is increasingly defined by uncertainty.

Confronting uncertainty demands increased agility, and agility can be enhanced by unlocking the power of information – making it visible, understandable, shared, and, above all, trusted. The security of our nation rests on being able to share information in an environment free from unnecessary limitations and constraints. In the past, we moved and shared information inside our agencies and departments or between them, but only if our specific needs were known. The interface for moving information had to be engineered ahead of time and the determination that someone might want or need the information had to be made well in advance. It was very difficult to share information on an ad-hoc basis.

Today, we produce data that is timely and useful to others, but predetermined formats must be used. Information can be made accessible and secure, but only if we stay within departmental boundaries and systems. Today, information collection and analysis is ready for posting, but only if you know where to find it. What if we could remove those obstacles and migrate to a completely net-centric information environment? What if we could shift from a culture of hoarding data to a culture that readily shares it? Imagine how much more effective we would be.

To transition to a sharing culture, national and Department of Defense (DoD) information sharing strategies and plans have been put in place to ensure interagency sharing of information. Within the DoD, our key goals have been to build the Net, populate the Net, operate the Net, and protect the Net across the enterprise.

I cannot overemphasize how vital information sharing is to our national leadership under all conditions. Network cyber-security and infrastructure are critical to our national economy and security. From the President to the warfighter, leading-edge information technology has made it possible for users to say, "I can get the information I need to perform my mission," and *that* is net-centric transformation.

We have to remember that we are stewards of government information – we don't own it – and we have a responsibility to share it.

The Honorable John G. Grimes
Sponsor

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.

> *"... 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 ..."*

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.

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, multidimensional 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 technologies 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

CNSS: Interagency Partnering to Protect Our National Security Systems

The Honorable John G. Grimes
Department of Defense Chief Information Officer

The CNSS performs the vital function of mobilizing the full, interagency National Security Community for the protection of telecommunications and information systems that support U.S. national security. This article describes recent strategic accomplishments of the CNSS and individual federal departments and agencies along with priorities for 2008.

The United States faces increasing threats in the homeland security, cyber security and information sharing environments, and the need for increased cooperation among key members of government, industry, academia, the private sector, and allied nations has never been greater. CNSS provides an interagency forum for addressing IA policy issues impacting critical NSS. Through its membership and partnerships (a total of 21 members and 10 observers from the executive branch of the U.S. government) the CNSS has a history of addressing vulnerabilities that have the potential to impact the national security community's ability to safeguard key systems. In 2007, the CNSS made significant contributions to federal, state, local, and coalition security efforts across the following five areas:

1. Assured Information Sharing (AIS)

AIS is fundamental to the integrity of our data and systems, and is essential to the nation's well-being and defense. The CNSS is actively engaged in making significant improvements across these areas. The UCDMO – a joint effort between the DoD and the DNI – has put out a unified technology road map to expedite the use of information sharing solutions between classification domains. The CNSS will extend the UCDMO's progress to other federal departments and agencies and improve information sharing among government departments and agencies. One of the key tools that revolutionized communications in recent years has been wireless devices such as PDAs and Blackberries. The emergence of the Secure Mobile Environment Portable Electronic Device – with e-mail and Web browsing capabilities up to the Secret level and voice capabilities up to Top Secret – is taking wireless to the next level. It will provide the homeland and national security communities with secure communications whenever and wherever they are needed. Another area the CNSS has emphasized is the use of data at rest encryption to protect sensitive unclassified data stored on removable media and mobile computing devices like laptops. Communication and information exchange between the U.S. and our allies in the global war on terror has been an area where the CNSS has been actively engaged. In 2007, the CNSS approved more than 60 transfers of critical products to improve information sharing. For 2008, CNSS priorities for AIS will highlight the need for developing and deploying more tools, technologies, and products that will ensure the national security community has secure, reliable access to information whenever and wherever it is needed.

> *"Access control based on standard user characteristics (like the user's organization or role) increases both speed and security when it comes to information sharing."*

2. Managing Risk

Assessing and managing risk is essential to safeguarding NSS, and we have a solid strategy to counter the threats posed by those who attempt to exploit vulnerabilities in the hardware and software we rely on. The CNSS is championing a common risk assessment methodology and a common C&A process across the government. These changes will help identify vulnerabilities, determine acceptable risk levels, and increase trust among system owners. The use of common approaches will improve capabilities, reduce costs, and increase interoperability. For the coming year our priorities for managing risk include establishing common approaches for C&A, risk assessment, and managing supply chain risk.

3. Identity Assurance

The majority of successful network penetrations today are due to failures in identity assurance where a compromised password and user ID have been used to gain unauthorized access. Establishing strong identification and authentication techniques for people and devices are central to any security effort, and that makes assurance critical. Access control based on standard user characteristics (such as the user's organization or role) increases both speed and security when it comes to information sharing. Members of the CNSS are working to promote the use of identity assurance technologies such as smart cards, tokens, biometrics, and public key technologies. Identity assurance priorities include expanding the public key infrastructure to additional communities of interest and leveraging other promising technologies such as biometrics.

4. Network Resilience for Mission Assurance

The global information infrastructure supporting the President, our military commanders, and homeland security leaders must be reliable and resilient even in the face of attacks. National security rests on having the confidence that these critical functions will be accessible during disrupted and distressed conditions. By working with private sector and allied partners, we ensure critical capabilities and missions remain operational.

CNSS Policy No. 12, issued in March 2007, emphasized integrating IA into the life-cycle of space systems that collect, generate, process, store, display, or transmit national security information. This was a huge step forward and had a dramatic impact on the commercial satellite assets so critical to keeping our networks resilient. Additional priorities for 2008 include national-level exercises to enhance responses to serious cyber-degradation by critical infrastructure owners/operators, accelerating next-generation security management infrastructure development, security capabilities supporting global information sharing, and increasing the focus on continuity of operations and reconstitution.

5. Building and Sustaining the IA Work Force

People are the most critical element in securing national security systems. They operate the technology, implement the procedures, execute the policies, and make the decisions that impact everything the CNSS touches. The IA professionals who build, maintain, and defend our critical networks deserve the best education and training possible, and the CNSS has established strict standards for national IA training and education to support them. These standards have been incorporated into the training curriculum at more than 160 institutions in government, academia, and the private sector. In 2007, more than 80 centers of academic excellence across 34 states and the District of Columbia provided college students with high-level IA education, along with the opportunity to earn federal scholarships. Many scholarship students are now working for the federal government where their IA expertise is contributing to the security of our national information infrastructure. CNSS priorities for 2008 include improving IA education nationwide and working more closely with private sector training and certification vendors to infuse standards into their certification programs.

As the CNSS Chair, I am proud to say it continues to be an invaluable interagency forum for engaging the national security community on long-term, integrated solutions so vital to protecting the global information infrastructure. CNSS priorities for 2008 support the President's national cyber-security initiative, and focus on increasing the level of trust in NSSs, protecting them from our adversaries and making certain that mission-essential functions can be performed in an increasingly hostile cyber-environment. The complex challenges and emerging issues brought to the forefront by this invaluable group not only delivered benefits for national security, they also created a ripple effect that touches countless other functional areas and communities.◆

About the Author

The Honorable John G. Grimes was nominated by President Bush on June 17, 2005 and sworn in as the Assistant Secretary of Defense for Networks and Information Integration/DoD CIO on November 14, 2005. He has extensive technical and policy experience in telecommunications, information systems, and the command and control fields. Grimes' public service includes the White House National Security Council Staff as Director for National Security Telecommunications Policy; Director of Defense Command, Control and Communications Programs; and Senior Director White House Situation Support Staff. He served as Deputy Assistant Secretary of Defense for Defense-wide Command, Control, and Communications and was the Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures. As a member of the DoD senior executive service, Grimes held senior technical and staff positions with the National Communications System; Defense Communications Agency; and the U.S. Army Communications Command following his military service in the U.S. Air Force. Previously with Raytheon, he served as Vice President of Intelligence and Information Systems, Washington Operations. Grimes has served on four Defense Science Board Task Forces and was a member of the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee. Grimes is a graduate of the University of Arizona, and has a master's degree from Shippensburg University in Pennsylvania. He is a graduate of the U.S. Army War College, Carlisle Barracks, Pennsylvania; the Federal Executive Institute, Charlottesville, Virginia; and Harvard University's National and International Security Policy program. He is the recipient of the American Institute of Aeronautics and Astronautics' Command, Control, Communications, and Intelligence award among other public, military and federal civil service awards, including two Presidential Rank awards.

6000 Defense Pentagon
Washington, D.C. 20301-6000

Coming Events

August 4-7
2nd IEEE International Conference on Semantic Computing
Santa Clara, CA
http://icsc.eecs.uci.edu/index.html

August 11-15
Integrated Systems Health Management Conference
Covington, KY
www.usasymposium.com/ishm/default.htm

August 18-20
The 10th IASTED International Conference on Signal and Image Processing
Kailua-Kona, HI
www.iasted.org/conferences/home-623.html

August 18-21
Guidance, Navigation and Control Conference
Honolulu, HI
www.aiaa.org

August 25-28
COMSEC Managers Conference
Boston, MA
www.nsa.gov

August 25-28
Implementation Fest 2008
Lake Buena Vista, FL
www.adlnet.gov

September 15-18
4th World Congress for Software Quality
Bethesda, MD
www.asq.org/conferences/wcsq

2009

STC Systems & Software Technology Conference

2009 Systems and Software Technology Conference
Salt Lake City, UT
www.sstc-online.org

Coming Events: **Please submit coming events that are of interest to our readers at least 90 days before registration. E-mail announcements to: nicole.kentta@hill.af.mil.**

Making GIG Information Assurance Better Through Portfolio Management

Thomas E. Anderson
GIG Information Assurance Portfolio Management Office

Within the federal government, IT portfolio management (PfM) emerged as a fundamental business imperative driven by legislation such as the Clinger Cohen Act (CCA) [1] *of 1996, which called for greater accountability for performance and expenditures. In addition to providing guidance to the federal government on how to improve the management and allocation of its investments, CCA also changed the organizational structure and behavior of the government, vesting more power in its CIOs. This article provides insight into how the DoD CIO has approached PfM for IA within the GIG.*

In October 2005, the Deputy Secretary of Defense signed out DoD Directive (DoDD) 8115.01, "Information Technology Portfolio Management" [2], which established policy and assigned responsibilities for the management of DoD IT investments as portfolios that focus on improving DoD capabilities and mission outcomes. Under the directive, the responsibility of establishing guidance for managing portfolios was placed with the ASD[NII]/DoD CIO. Individual portfolios manage their investments using strategic plans, GIG architecture, risk management techniques, and capability goals, objectives, and performance measures.

As the benefits of PfM have become more widely recognized, the DoD is moving toward the management of all investments (not just IT) as portfolios. The 2005 Quadrennial Defense Review initiated a process that has piloted Capability Portfolio Management (CPM) and specified a structure whereby capabilities will be managed in a series of portfolios. The DoD is preparing to issue an overarching policy to formalize a comprehensive DoD CPM framework based on the Joint Capability Area taxonomy. To avoid the confusion of having two portfolio processes within the DoD, the DoDD 8115.01, "Information Technology PfM," will be canceled when the new CPM policy is issued. The policies currently contained in DoD Instruction 8115.02, "Information Technology PfM Implementation," will be updated to support the CPM framework and fully merge portfolio governance structures.

Under this new framework, capability portfolio managers will make recommendations to the Deputy Secretary of Defense and the Deputy's Advisory Working Group on capability development issues within their respective portfolios. They have no independent decision-making authority and will not infringe on any existing statutory authorities. For instance, the DoD CIO's statutory and regulatory responsibilities to manage and oversee IT resources remain unchanged; however, they will now be executed through this more holistic portfolio structure. In essence, capability portfolio managers integrate, coordinate, and synchronize portfolio content by providing strategic advice intended to focus portfolio capabilities.

> *"Traditionally in both the commercial sector and the federal government, PfM has focused on IT-related investments, but in an ideal world, the portfolio should be inclusive of all investments: people, processes, and technology."*

What Is PfM?

PfM is the management of selected groupings of investments through integrated strategic planning, architecture, measures of performance, risk-management techniques, and transition plans. Traditionally in both the commercial sector and the federal government, PfM has focused on IT-related investments, but in an ideal world, the portfolio should be inclusive of all investments: people, processes, and technology. In the simplest and most practical terms, PfM focuses on five key objectives:

1. **Define goals and objectives.** Clearly articulate what the portfolio is expected to achieve. What is the mission of the organization and how does it support and achieve that mission?
2. **Understand, accept, and make trade-offs.** Determine what to invest in and how much to invest. Which initiatives contribute the most to the mission?
3. **Identify, eliminate, minimize, and diversify risk.** Select a mix of investments that will avoid undue risk, will not exceed acceptable risk tolerance levels, and will spread risks across projects and initiatives to minimize adverse impacts. When and how do you terminate a legacy system? At what point do you cancel a project that is behind schedule and over budget?
4. **Monitor portfolio performance.** Understand the progress your portfolio is making towards achieving the goals and objectives of your organization. As a whole, is the portfolio's progress meeting the mission's goals?
5. **Achieve a desired objective.** Have the confidence that the desired outcome will likely be achieved given the aggregate of investments that are made. Which combination of investments best supports the desired outcome?

What Is the GIG?

Everyone hears about the GIG, but just what is it? The DoD defines the GIG as the following:

> ... a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information.

The GIG will improve interoperability among the DoD's many information and weapon systems, but more importantly, it

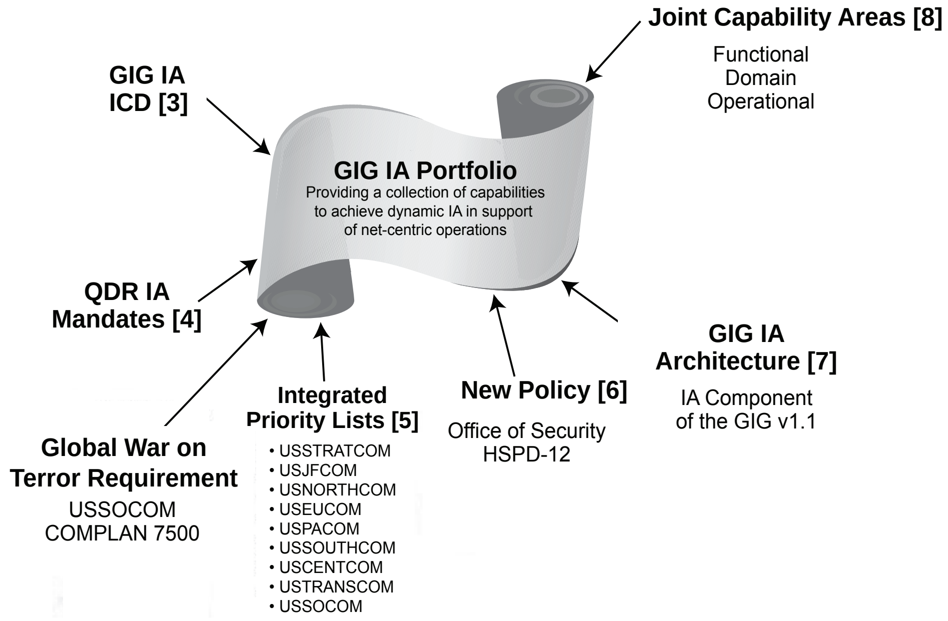


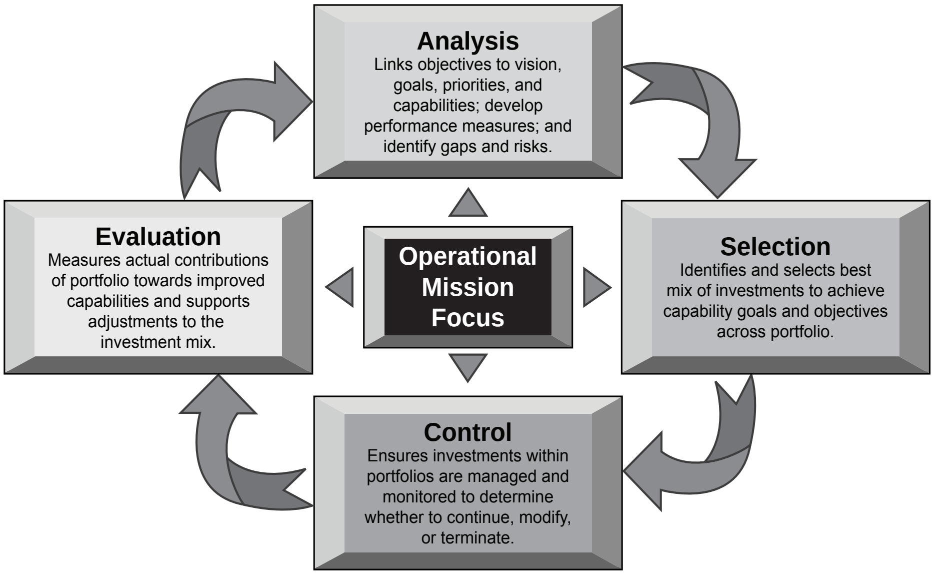
Figure 1: *GIG IA Portfolio Drivers*

will help the DoD to transform to a more network-based – or net-centric – way of fighting wars and achieving information superiority over adversaries, much the same way as the Internet has transformed industry and society on a global scale.

The GIG will create an environment in which users can access data on demand from any location without having to rely on (and wait for) organizations in charge of data collection to fully process and disseminate the information. With its timelier data availability and more robust communications infrastructure, the DoD expects the GIG to enable more expedient execution of military operations, collaborative mission planning and execution, and common views of the battlespace. The realization of the net-centric vision depends on sound IA mechanisms being woven into the very fabric of the GIG. Reaching the GIG vision relies to a great extent upon each individual program manager understanding and being willing to be guided by the tenets of the GIG. Applying the tenants of PfM, the strategy for weaving IA into the GIG, consequently, has three main prongs:

1. Developing and operationalizing an IA component of the GIG architecture that provides the technical road map for protecting and defending the current and future GIG.
2. Influencing program managers to build their systems so as to be able to plug into relevant IA constructs.
3. Ensuring the DoD makes the proper investments to provide the IA foundational technology upon which the programs will be relying.

Figure 2: *PfM Process*


Analysis
Links objectives to vision, goals, priorities, and capabilities; develop performance measures; and identify gaps and risks.
Evaluation
Measures actual contributions of portfolio towards improved capabilities and supports adjustments to the investment mix.
Operational
Mission
Focus
Selection
Identifies and selects best mix of investments to achieve capability goals and objectives across portfolio.
Control
Ensures investments within portfolios are managed and monitored to determine whether to continue, modify, or terminate.

What Is GIAP?

The ASD(NII)/DoD CIO named the DASD(IIA) as the domain owner for the IA Portfolio who, in turn, named the Director, National Security Agency (DIRNSA) as his domain agent. As the IA domain agent, the DIRNSA leads the GIAP management activities through the creation of the GIAP Management Office.

The GIAP Management Office consists of a GIG IA portfolio manager and staff of capability managers who execute the domain agent duties on behalf of the DIRNSA. Though located at the NSA, this office performs a DoD community service and draws staff from across the community. At present, the GIAP Management Office workforce consists of NSA and DISA personnel.

Key IA organizations have been appointed as functional leads to support the IA domain agent in developing and executing a coordinated, DoD-wide IA portfolio. The functional leads are:

- Architecture – NSA IA Directorate.
- Integration – DISA.
- Operations – Commander, U.S. Strategic Command.
- PfM – GIAP Management Office.

So Why Have a GIAP?

As the domain owner, the DASD(IIA) has directed the GIAP Management Office to provide a collection of capabilities that will achieve dynamic IA in support of net-centric operations. The primary focus of the GIAP Management Office is to do the following:

- Recommend the best mix of investments, and synchronize milestones and dependencies to achieve the GIG IA vision.
- Fully leverage baseline resources from research to de-commission.
- Identify approaches to close all capability gaps.
- Monitor execution of investment strategies.
- Measure outcomes and processes and take corrective measures as necessary.

The GIAP Management Office does not manage the execution of service and agency IA programs as this is the responsibility of the services and agencies themselves. The GIAP Management Office closely examines the programs to understand capabilities on which they are depending for their success. They also look at the timing of the programs to ensure they are synchronized logically.

The GIG IA portfolio manager, in concert with the capability managers and service/agency representatives, has been working hard to meet these goals. Figure 1 depicts the many drivers of the GIAP in its goal to provide a collection of capabilities that will achieve dynamic IA in support of net-centric operations.

Division of the GIAP Into Capability Areas

In order to aid the GIAP manager in the task of delivering GIG IA capabilities to DoD customers, the GIAP has been divided into six distinct IA functional areas under the direction of four capability managers. These six IA functional areas are aligned to do the following:

1. Provide the ability to dynamically and securely share information at multiple classification levels among U.S., allied, and coalition forces.
2. Protect all enterprise management and control systems, and provide common security management infrastructure to support enterprise security functions.
3. Provide assurance that information does not change (unless authorized) from production to consumption or from transmission to receipt.
4. Protect, monitor, analyze, detect, and respond to unauthorized activity as well as unintentional, non-malicious user errors within DoD information systems and networks.
5. Assure GIG computing and communications resources, services, and information are available and accessible to support net-centric operations.
6. Ensure information is not made available or is not disclosed to unauthorized individuals, entities, devices, or processes.

The capability managers are responsible for providing oversight and guidance to all DoD programs delivering capabilities within their functional area. They work closely with the services and agencies managing these programs, with the functional leads, and with each other. In providing this oversight and guidance, they follow the process depicted in Figure 2.

Supporting the PfM process described in Figure 2, the GIAP has developed the GIG IA Portfolio Plan (GIPP) which sets forth a near-term plan in the context of a long-term vision for fulfilling GIG IA-identified capability gaps defined in the GIG IA Initial Capabilities Document (ICD) [3]. While describing the long-term vision at a high level, this version of the GIPP is particularly focused on presenting a plan to achieve the capabilities defined in the IA component of the GIG Integrated Architecture, Increment 1, Version 1.1 [7]. The GIPP also serves as a guide for the GIAP in determining recommendations for the best mix of synchronized investments over time, and serves to inform the community of the near-term plan for investments and the expected availability of capabilities. The GIPP communicates the GIAP path by doing the following:

- Defining architecturally framed technology evolution strategies.
- Providing practical details that describe implementation progress necessary to counter adversaries, close gaps and vulnerabilities, and achieve net-centricity.
- Identifying programmatic dependencies and synchronization markers.

> *"Beyond cost, schedule, and dependencies, analyses will continue to identify possible duplication of effort by one service or agency which could be used by all. Achieving the GIG vision ... will not come quickly ..."*

What Lies Ahead

The GIAP Management Office has a huge task before it – one that will take several years to fully implement. Since its establishment in 2006, the GIG IA PfM office's near-term focus has been on issuing guidance to the services and agencies to help them refine their Program Objective Memorandum '08 and '10 submissions, plan their fiscal year '09-13 budget and, where possible, modify their fiscal year '07-08 budgets. Beyond cost, schedule, and dependencies, analyses will continue to identify possible duplication of effort by one service or agency which could be used by all. Achieving the GIG vision and associated IA architecture will not come quickly and will not be cheap, but through PfM we can maximize our investment by ensuring that scarce IA dollars are spent as wisely as possible. As our insight into ever-changing adversarial threats deepens, PfM gives us the agility to plan, budget, and support capability improvements necessary to sustain an assured GIG into the future by providing the best IA to the warfighting and ICs.◆

References

1. CCA <www.defenselink.mil/cio-nii/docs/ciodesrefvolone.pdf>.
2. DoDD 8115.1. IT PfM <www.dtic.mil/whs/directives/corres/html/811501.htm>.
3. GIG IA ICD <www.cryptomod.org>.
4. Quadrennial Defense Review Mandates <http://defenselink.mil/gdr/report.pdf>.
5. Integrated Priority List <www.dtic.mil/doctrine/jel/doddict/data/i/02725.html>.
6. Homeland Security Presidential Directive 12 <www.whitehouse.gov/news/releases/2004/08/20040827-8.html>.
7. IA Component of the GIG Integrated Architecture Increment 1, Version 1.1 <www.us.army.mil/suite/folder/9714582>.
8. Joint Capability Areas <www.dtic.mil/futurejointwarfare/cap_areas.htm>.

About the Author

Thomas E. Anderson is currently the Deputy Chief of the GIAP Management Office within the NSA's IA Directorate. Before his appointment to his current position, Anderson served as the Chief of the Technology and Capabilities Division of the DIAP within the Office of the DASD(IIA), OASD(NII)/DoD CIO. During his tenure at the NSA, Anderson held numerous positions supporting the evaluation of commercial off-the-shelf products and the establishment of the National Information Assurance Partnership between the NSA and the National Institute of Standards and Technology. Prior to joining NSA, Anderson retired from the U.S. Army after 20 years of service. Upon his retirement from the Army and prior to joining the NSA, Anderson worked as an INFOSEC engineer.

E-mail: t.anders@radium.ncsc.mil

Information and Communications Technology and the Global Marketplace

The DoD Globalization Task Force Staff

The global information and communications technology (ICT) marketplace brings innumerable benefits to the USG and DoD. However, this extended and often unknown supply chain has created an environment where trustworthiness in commercial ICT products is no longer implicit, requiring the USG to expand its understanding of IA. In this new environment, employing comprehensive protection mechanisms requires consideration of both the depth and breadth of the approach; that is, risk and risk mitigation must be considered across the entire lifecycle of the product or system, from requirements development to retirement. The DoD is working to develop solutions to manage risk at the network, systems, and product level. Potential solutions include partnership with industry in supply chain oversight and standardization to facilitate keeping intruders and malware out of USG and DoD networks.

The impact of the global marketplace on USG IA activities and technology acquisitions is permanent, irreversible, and likely to have only greater impact over time. In order to stay on the cutting edge of technology development, the USG and its commercial supplier base must rely on industry partners from around the world. And, with increasing frequency, it is foreign companies that are providing the most advanced technology solutions. The multi-tiered, global nature of our supply chain means that the government has suppliers that it may not know and may never see. With less insight into their security practices and less control over how they conduct their business, this global supply chain may make the USG more vulnerable to an adversary who can use security gaps in our global supply chain against us.

Our traditional defense approach, *defense-in-depth*, as defined by DoDD 8500.01E, focuses on the following:

> ... establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among information technology assets; and, the selection of IA solutions based on their relative level of robustness. [1]

This approach implies a degree of trustworthiness in commercial ICT. However, trustworthiness in commercial ICT products is no longer implicit. A new defensive strategy, *defense-in-breadth*, is necessary to complement our traditional approach and manage risk over the lifecycle of a network, system, or product.

The comforting assumptions the DoD and the broader USG have had about their suppliers are no longer true – especially in the ICT industry. No industry has been more transformed by globalization than the ICT industry. Today, ICT – including micro-electronics [2] and software [3] – is being developed around the world. Companies may be headquartered in the United States but perform much of their research and development, manufacturing, and servicing in China, India, or numerous other countries. In addition, these companies contract out work to multiple subcontractors whose processes and practices are often unknown. Even for the decreasing number of ICT firms that are largely based in the United States, much of their talent may come from abroad.

“... with a much more transitory, global, and permeable supply chain, trustworthiness in our ICT is no longer a guarantee – even from our American companies.”

This picture of a truly international industry contrasts sharply with the supplier base that the DoD and other USG agencies dealt with in the past. They were able to count on companies here in the United States with domestic research, manufacturing facilities, and American employees. Moreover, the government could be confident that these *all-American* companies were developing the cutting-edge technologies that underlay so much of American strategic dominance. These were firms whose products they could trust. However, with a much more transitory, global, and permeable supply chain, trustworthiness in our ICT is no longer a guarantee – even from our American companies.

There is no way to go back to a supplier base of all-American companies. While some departments do, for extraordinary reasons, build proprietary technology for government use using a cleared facility and cleared personnel, this approach is neither ideal nor financially feasible on a large scale for the bulk of the purposes for which ICT is intended. Business practices and the worldwide development of technology make the old ways impossible.

First, globalization optimizes resource use and improves the efficiency of production and distribution. Now, a team of developers in California can stop work and hand off their project to a team in Europe, which can, in turn, hand off to a team in Asia – making for a 24-hour development day. Moreover, those foreign developers are highly competent, are able to provide insight into the requirements of foreign markets, and can produce a competitive advantage in the U.S. market.

Also, the supply chain itself complicates the USG's ability to ensure the trustworthiness of products purchased from the global marketplace. Lean manufacturing processes and just-in-time operations exacerbate the lack of control, limit transparency, and inhibit the ability to inject security into the process. In a highly competitive environment, security testing may be minimized because the cost and time required are hard to absorb.

The national security concern regarding the global marketplace is that software or microelectronic circuitry may include deliberately inserted malicious logic – *malware* – that an adversary might slip into a computer system to steal or corrupt data or disrupt the system. The malware might act immediately or it may be designed to lie dormant until activated by some future signal. Buried in the millions of lines of code that comprise the modern computer application, such malware is difficult to detect even with desktop-level malware applications such as Symantec: no one may be aware of its existence until after the damage is done.

For example, it was reported in Britain's *Channel Register* in November, 2007 [4] that hard-disk drives built for a U.S. data storage company by a Chinese subcontractor were infected with a Trojan horse virus named AutoRun-AH, which searches for passwords to online games and sends them to a server located in China. Although the company acted promptly upon the discovery of the malware, some units were sold to the public before it became aware of the compromise.

While compromising ICT may not be as easy a way to penetrate a computer system as hacking into it or turning an insider, it is a viable option for a determined adversary. Moreover, to the extent security measures make hacking more difficult or subversion more challenging, infiltrating the supply chain becomes a more attractive alternative.

There is no single – nor quick – fix for mitigating the risk to DoD and USG systems and networks stemming from the global ICT marketplace; yet the problem is not an impossible one to manage through a defense-in-breadth. The risks associated with a globalized supply chain can be addressed if one understands the problem, makes a concerted effort to address threats and vulnerabilities at key points over the life of ICT products and systems, and partners with commercial providers to improve the integrity of ICT products. Depending on the level of risk to the system or network, the mission area, and available capabilities, different systems and networks will require different combinations of risk management techniques. For national security computer systems, that effort is, therefore, going to be far more extensive than for another buyer with a less sensitive system – the challenge for any user is to select a mix of options that is cost-effective.

Both suppliers and acquirers have to be aware of the risk. Many government agencies and companies are beginning to rethink the implications of globalization on their supplier base. Neither they nor the sellers may have been sensitive to the possibilities of supply chain vulnerabilities in the past. No one is going to act unless they understand that there is a problem, and that level of awareness is only now developing.

One useful step will be for ICT suppliers to develop and maintain practices and procedures that monitor the development process in both their own facilities and those of any subcontractor that they use. Processes and tools that track when source code or hardware is accessed, who accesses it, and what changes they have made raise confidence. Similarly, strong business processes managing reputability and quality of components incorporated into ICT help bound risk. Commercial standards in this area clarifying commercial best practice regarding configuration management, design, and quality control in the presence of global sourcing can enable the systems' acquirers to express requirements and bound risk that unanticipated code or components have been placed within a reputable developer's configuration.

> ***"Buyers and testing labs have tested the functionality of software and hardware for many years – ensuring it does what it promises – but they have not been as focused on testing for security."***

The adoption of such standards and best practices will proceed only if acquirers recognize their importance, require that suppliers adhere to these security processes, and recognize that a low-cost, low-security supplier can present a much higher cost in the long run. Those with the knowledge to create standards will likely do so only if there is genuine pressure from the larger buyer community to get it done.

However, at the time of purchase, a user may face a troublesome reality: even for those that have adopted all the standards and best practices required, there is no complete assurance that the product is trustworthy. Here, users must be more vigorous and sophisticated in protecting themselves. They have to evaluate the residual risk arising from the ICT that they are about to purchase and decide what steps they can take to configure their own systems to minimize that risk. The financial industry and some government agencies have been developing best practices to employ to counter this residual threat. The practices are tailored to the level of risk and the importance of the system, but the challenge will be to adapt enduring security controls in light of continuous technology changes, such as software updates, and shifts in an adversary's tactics.

One might ask if the entire problem could be solved by simply testing all that code to see if it contains malware. That is easier said than done. Buyers and testing labs have tested the functionality of software and hardware for many years – ensuring it does what it promises – but they have not been as focused on testing for security. It has traditionally been easier to test functionality than security, and the gap between the two has only grown as applications have become more complex. Even if the problem could ultimately be solved by testing, no such test is currently on the horizon. In its September 2007 report on Mission Impact of Foreign Influence on DoD Software, the Defense Science Board (DSB) recommended that the DoD fund science and technology research and development in state-of-the-art software and hardware vulnerability detection and mitigation [1]. The DSB highlighted the desired outcomes of this R&D as developing technology to eliminate accidental vulnerabilities from systems development and to improve trusted computing group technologies to mitigate the risks posed by malicious software [5].

The Cyber Security Research and Development Act (CSRDA) of 2002 [6] is one possible means of supporting the development of better tools. The CSRDA was signed into law November 27, 2002, to enable the U.S. to prepare against cyber-attacks on federal and private computers. The act directs the National Science Foundation to establish cyber-security research centers, community college grants, fellowships and undergraduate program grants, partnerships with industry and academia, and the establishment of a program to encourage senior researchers in various fields to transition to work in computer security [7]. The CSRDA authorized more than $900 million over five years for R&D and training programs by the NSF and the National Intelligence Support Team. However, it is not clear how much time and money it will take to create new tools – and there is no guarantee that they will be able to keep up with the continually increasing complexity of the products they are reviewing.

There is one thing that is not part of the solution. There is no value in simply *banning* software or hardware manufactured in any particular country. Such a ban assumes that somehow the problem is geographically focused. It is not. Such a ban would not only raise questions under the rules of the World Trade Organization, but would also disrupt the ongoing operations of numerous legitimate U.S. and foreign companies that have come to rely upon work products from various overseas resources. Moreover, it would give a false confidence to buyers who might assume that merely because a product was produced in the U.S., for example, it should be secure.

Instead, the USG must reach out to global commercial partners to improve the state of play. Government cannot solve the problem without industry's help, and industry stands to benefit from dealing with the problem of supply chain risk in many ways. ICT providers need to be able to assure all of their customers, not just those with national security concerns, that the product being provided is genuinely secure. A widespread fear among buyers that there might be malware in their new software, for example, would depress sales and tarnish a brand. One only need recall the recent problems with lead paint on toys from China to understand the potentially devastating impact of a malware scare on software products.

An analogous problem facing commercial ICT developers is the reliability concern stemming from the increasing circulation of counterfeit commercial components. The globalization of the marketplace has led to commercial collaboration among widely diverse cultures, including those for whom respect for intellectual property is an emerging concept. This situation has led to a significant problem of counterfeit ICT component parts and products, often developed without quality or security best practices, appearing in critical systems and networks.

The heightened awareness of more general security issues associated with the Internet and software has led to increased emphasis on information security. Increased use of intrusion detection devices and other controls will likely have some benefit with regard to supply chain risks as well as those that come from more typical problems such as hacking, but more must be done.

The DoD is committed to managing the risk presented by globalization using defense-in-breadth: a multi-faceted, risk-mitigation strategy that seeks to identify, manage, and eliminate risk at every stage of the IT system or network lifecycle, from system requirements generation to system retirement. It is actively working to ensure that policies and processes are put in place to raise awareness of the risk, empower acquirers to make informed decisions when they request and procure ICT products and services, and arm acquirers with practices and tools necessary to mitigate risk when ICT products are used across the government (the more traditional defense-in-depth component). It is also partnering with the commercial companies that comprise its supply chain and using its power as a consumer to drive security-minded attributes into the development and management of new systems and technologies. Both government and industry stand to lose if the risk presented by globalization of the ICT supply chain is not managed effectively. Our adversaries' exploitation of vulnerabilities in the ICT supply chains have the potential to threaten our national and economic security by putting sensitive USG and corporate information at risk and generating distrust in the security of ICT products. The DoD cannot solve this problem without help from its partners both in government and industry.◆

References

1. Department of Defense Directive 8500.01E. "Information Assurance." 24 Oct. 2002 <www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>.
2. Defense Science Board. Report of the Defense Science Board Task Force on High Performance Microchip Supply. Washington: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. Feb. 2005.
3. Defense Science Board. Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software. Washington: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. Sept. 2007.
4. Leyden, John. "Chinese Trojan on Maxtor HDDs Spooks Taiwan." Channel Register. 12 Nov. 2007 <www.channelregister.co.uk/2007/11/12/maxtor_infected_hdd_updated>.
5. Defense Science Board. Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software. Washington: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. Sept. 2007.
6. Pub. L. Cyber Security Research and Development Act. Nov. 2002.
7. GovTrack.us. "H.R. 3394 107th Congress (2001): Cyber Security Research and Development Act." GovTrack.us <www.govtrack.us/congress/bill.xpd?bill=h107-3394>.

About the Author

Mitchell Komaroff leads and is the Acting Director of the Globalization Task Force (GTF), for the ASD(NII)/DoD CIO. The GTF is an office within the Office of the DoD CIO dedicated to strategic national security planning to address risks arising from the globalization of the telecommunications infrastructure and of the marketplace for information and communications technology. He is primarily responsible for developing and implementing a strategy for mitigating national security risks to DoD arising from the increasing globalization of the ICT sector. The GTF is the ASD (NII)/DoD CIO focal point for transactional risk management in Committee on Foreign Investment in the U.S. and Federal Communications Commission licensing matters, developing strategies for preserving and improving Internet security and stability in support of DoD and USG communications, and policy development addressing global supply chain risk. Komaroff has worked to implement software and systems assurance across the DoD. He has worked previously as a computer scientist with DISA, and with industry where he worked network quality of service, IA architecture, and information management issues. Komaroff holds a master's degree in mathematics from George Mason University and a Juris Doctor degree from the University of Maryland, School of Law.

Phone: (703) 697-3314
E-mail: mitchell.komaroff@osd.mil

The Future of the Internet

The DoD Globalization Task Force Staff

The Internet's continuing growth, stability, and security are vital to the DoD's mission. While the DoD no longer controls Internet decision making, its unique perspective deriving from its multiple roles as Internet user, operator, and research center is important to the development and protection of U.S. national interests. It should make a commitment to participate directly in international Internet decision-making forums, as well as actively develop policy as part of the U.S. interagency process.

The Internet is essential. It is a vital underpinning of the civilian economy, and its security and stability has become a matter of national security. In a converged world, it will become not just the means for transmitting data, but also video and voice. It is, therefore, critical to ensure its continued growth, internal security, and stability.

So how do we guarantee that growth, security, and stability? What might impact those issues? Who gets to make those decisions?

The USG, through the DoD, created the Internet, but what it created has grown in ways totally unforeseen just 10-15 years ago. The DoD's oversight of the initial development of the Internet has been replaced by a web of collective decision-making bodies that it no longer controls. The issue now has become should the DoD continue to try to influence the development of the Internet and, if so, how should it proceed? That is, should the DoD take an active role in the process and, if it should, will that role be confined to internal USG deliberations or will it include direct participation in the many forums where key decisions about the Internet are made?

The rest of this article answers that question as follows: the DoD finds itself in a unique position to play a positive role. It is a major user of the Internet, but it is also a large Internet service provider and an operator of two of the 13 root zone servers that provide the basic information for locating Internet addresses. The DoD is also a repository of vast technical expertise about the Internet and a significant source of research funds. Taken together, those multiple roles give the DoD a unique view of the Internet and a distinct ability to positively influence its evolution in ways not easily matched by other USG departments or the private sector.

Those perspectives – individually and in combination – are critical for the DoD to carry out its larger mission: assuring the security and stability of the Internet as part of its defense of U.S. national security. The DoD's strategy should be twofold. It must (1) monitor and influence current technical and political developments that could impact the security and stability of Internet operations; and (2) envision the Internet 10 or 15 years into the future, define the role it will play in contributing to the defense of the nation, and take the steps required to achieve that vision, much as the defense community has done with the current Internet.

However, the DoD's distinct vision does not mean that it can afford to act alone. In order to make the DoD's participation effective, there will have to be a coordinated strategy among the DoD's components, as well as collaboration with the rest of the USG and the U.S. private sector. That collaboration is not driven merely by the desire to speak with one voice. Rather, it is compelled by the unique set of problems and unique ways of solving them that distinguish the Internet and its governance processes.

Collective decision-making about the Internet is disbursed among various organizations and, in most of them, governments have no special role. They stand on equal footing with the private sector, academia and civil society in devising standards and making other relevant decisions. It is a *megacommunity*[1] of extraordinary scope with vast and complicated interests and connections.

Moreover, the decision makers must constantly struggle to preserve the Internet's grassroots innovation and growth while recognizing the importance of stability and security. The creativity that has made the Internet so valuable cannot be squelched if the Internet is to remain a dynamic and adaptive medium. Continuing to achieve that balance of innovation and stability requires a combination of technological expertise, political sophistication, and a commitment to innovation and change that few individuals, let alone agencies, possess. It is the combination of perspectives from within and outside of government that, if successfully executed, gives the USG both compelling influence and a powerful vision.

The Questions

The following questions are integral to an Internet Governance and Security Strategy for the defense community:

- What should the Internet look like in 10 or 20 years to ensure it remains a secure link to our allies, the defense community global supply chain, and the civilian infrastructure on which the USG depends?
- What should the Internet look like in 10 or 20 years to maximize its ability to support other USG interests?
- What steps should the national security community take today to ensure that the security and stability of the Internet's infrastructure are protected to support future operations? From a policy standpoint (i.e., global, national, DoD)? From an investment standpoint (e.g., resourcing, research and development)? From a cultural standpoint (e.g., training, education)? From a tactical standpoint (e.g., standards, operations, acquisitions)?

The Trends

One can likely come up with a variety of ways of categorizing the various challenges for the Internet. The following are three that are seen as summarizing the diverse problems:

1. The rapid *growth* of Internet services and, therefore, Internet traffic because of the increasingly essential character of the Internet for national and international economies (all of which makes the Internet not just a bigger target, but also a more inviting one, as well).

2. The growing sophistication of those who want to destroy the Internet's *stability and security*, whether for reasons of cyber-war, crime, or simple malicious one-upmanship.
3. The increasing demands placed on those *organizations* that make decisions related to standards and practices governing the Internet.

Growth

First, with regard to growth, the trends are overwhelming:

- Everything will be over Internet Protocol (IP) (Voice over IP [VoIP], video, streaming video, collaboration, data), which means systems will bear vastly greater amounts of traffic.
- Everything will be addressable via IP addresses (sensors, mission-critical systems, individuals, etc.).
- There will be vast numbers of new uses which will have implications on the volume of traffic and privacy of data, among other things.
- The Internet will be more intelligent and interactive.

That growth suggests a responsive agenda that should address the following areas:

1. **Scale/Ubiquity**. The more Internet traffic, the greater the threat of congestion and packet loss. The greater the congestion, the greater the interference with VoIP and video. Unlike data where we have learned to tolerate the time it sometimes takes for things to appear on computer screens (as we expectantly peer at our monitors), video and VoIP transmissions cannot be delayed or disrupted without substantially degrading service (which is referred to as the problem of *latency*). There are also questions of whether computational capacity on root zone servers can meet demand, and whether the constant updating of routing tables will strain the routers' computational ability. The routing schemes will need to account for more routers and links, and quality of service (a term related to the issue of *net neutrality*, discussed in the third area, Quality of Service) will complicate their work. Modifications to the current global routing scheme will be required to support controlled peering among networks, and routing protocols will need a complete system view of options (rather than a partial view focused on the next jump). There is also the question of whether increasing capacity requirements will be met with current technologies.
2. **Resiliency.** Ubiquitous VoIP and similar high bandwidth, low latency applications, as well as increasing dependence on the Internet for mission-critical operations, require a more reliable and robust system. In the face of major man-made or natural disasters or deliberate attacks on the system, will there be enough robustness, redundancy, and accurate routing and address information to assure continued connectivity and speed? In addition, exchange point technology needs to be improved and there are robustness issues at major interconnection points including, among other things, a lack of redundancy.

> *" ... some commercial users are worried about possible abuse of priority schemes by service providers to discriminate in favor of some content or services over others ... The White House has stated that it sees no reason for net neutrality legislation; that the market will work itself out."*

3. **Quality of Service – Net Neutrality and Priority of Service.** On traditional telephone networks, carriers have evolved protocols for priority communications, a particularly important issue for national security and law enforcement. Thus far, the Internet has worked on a *best efforts* basis where all traffic is essentially treated the same. With more traffic and potential limits on capacity, it is important to ensure similar priority schemes. However, some commercial users are worried about possible abuse of priority schemes by service providers to discriminate in favor of some content or services over others. They have proposed net neutrality laws that could interfere with the ability to prioritize communications for national security/emergency preparedness purposes. The White House has stated that it sees no reason for net neutrality legislation; that the market will work itself out [1]. The Federal Communications Commission (FCC) is currently reviewing net neutrality through a notice of inquiry[2], and holding hearings on the issue in light of evidence that carriers may have been violating net neutrality principles.
4. **IPv6 Deployment.** As a result of the growth of the Internet, the addressing system must be expanded. IPv6 is a new addressing system that allows for billions more potential addresses than the current system, IPv4. Both the USG and private industry must be prepared for the transition to ensure that it occurs smoothly and that all IP addresses remain reachable. Because of the relatively large number of addresses that remain available in the U.S., there has thus far been little interest here in undertaking the necessary investment, even though the Office of Management and Budget has directed all USG agencies to complete the transition by June 2008[3]. While the DoD has moved forward, many U.S. agencies have not. However, the rest of the world is likely to want to push forward in the near future. At that point, the U.S. may have no choice; however, timely addressing of the transition is the best way to avoid a crisis.
5. **Alternative Technologies.** The National Academy of Sciences has noted that Internet research at this point is heavily incremental in nature, focusing on marginal improvements to the current structure.[4] There is little money or effort devoted to changing the fundamentals of the Internet. Regardless, there is always the possibility that some alternative technology will come along that will make the Internet outmoded in the same way the Internet has begun to make the Public Switched Telephone Network (PSTN) virtually obsolete. If funded, the National Science Foundation Global Environment for Network Innovations project[5], with which the DoD (principally through the

Defense Advanced Research Projects Agency [DARPA]) collaborates, will investigate new core functionality, new architectures and new network architecture theories, and build higher-level service abstractions.

6. **Web 2.0.** Some issues of growth relate to the evolution of Internet applications. The increasing sophistication of highly interactive Internet applications, often collectively referred to as Web 2.0, provide users with an expanding range of capabilities.[6] The DoD can and does use them, but the value to the DoD is nowhere as significant as the capability they afford non-nation state actors – such as terrorists – to use new and innovative ways to train terrorists (e.g., avatars), share information, recruit followers, and otherwise enhance their ability to conduct asymmetric warfare.

For all these issues, the DoD's perspective is extraordinary. It is the user who has a direct interest in all these problems, but it is far more than that. For example, it is an Internet service provider that has to adopt IPv6, and it is a research funding source that can influence long-term events. If all parts of the DoD are talking to one another, then it is a *feedback loop* unparalleled in the Internet world.

Stability and Security

If growth is deemed a *good* trend, then the second trend, the increasing sophistication of hackers, criminals, and state-sponsored cyber-warriors clearly represents the *bad* side of the following equation:

- Identity theft, fraud, unwanted e-mail, and other Internet abuses continue to grow.
- Because the Internet can originate virtually anywhere and can easily penetrate a national boundary, cyber-crime is both everywhere and nowhere all at the same time.
- Cyber-attackers have learned to manipulate hundreds, sometimes thousands, of computers to conduct coordinated attacks on a computer system (called *botnets*). These botnets have significantly facilitated large, broad-scale attacks on computer networks called distributed denial of service attacks (DDOS).
- In 2007, a large-scale attack on Estonia demonstrated the ability of sophisticated parties to disrupt large parts of a national economy through the use of DDOS.[7]
- The international world has been unable to agree on what cyber-crime is or how to deal with those who commit it. The Internet Cyber-Crime Convention has been signed by only 43 countries, including the United States. Russia, China, North Korea, and many others have not signed.

There are many possible responses to these problems, but the following are clear priorities:

1. **DDOS.** DDOS attacks are increasingly being used to conduct attacks against key Internet assets including the Internet's root zone servers. These DDOS attacks attempt to overwhelm servers with vast numbers of messages. The use of botnets has increased the effectiveness of DDOS attacks. The last major attack in the U.S. occurred on February 6, 2007. Its impact was heavily mitigated by the use of any-cast technology, which, by duplicating root zone data bases on multiple servers around the world, allowed traffic to be re-directed around the victimized servers. However, the attackers are also growing more sophisticated, and the need for ever-more elaborate defense continues to grow. Mitigation approaches include bandwidth upgrades, ingress and egress filtering, and mandatory hardware configuration to eliminate the possibility that computers could be taken over by unauthorized users. One sign of the seriousness of the problem is that Internet service providers are considering the cost effectiveness of accepting only traffic from known entities. However, this approach could block access to online sites and eliminate the end-to-end nature of the Internet. Government and private industry will need to continue to work closely to address this issue from both a policy and operational perspective.

> *"The BGP is used to perform inter-domain routing on the Internet and is vulnerable to spoofing and misconfiguration, which can lead to the misrouting of Internet traffic."*

2. **Defining Cyber-War and Cyber-Conflict.** The Estonia situation showed the difficulties present in defining cyber-conflict. Although a nation-state was suspected of causing the DDOS attacks against Estonia's key Web resources, it was difficult to trace ultimate culpability. In addition, there was a question of whether this type of denial of service would be considered a cyber-incident of national significance considering the fact that it caused more annoyance than actual harm. Although the Estonia situation seemed to bring attention to the fact that nation-state strategic cyber activity might be on the rise, it equally brought light to the fact that cyber rules of engagement have yet to be defined. Much work will have to be done in the next decade defining international law and norms of behavior, by treaty or other means, to ensure that the Internet will survive in light of a rise in nation-state cyber conflict.
3. **Authentication (Public Key Infrastructure/Domain Name System [DNS] Security Extension [DNSSEC] Deployment).** To ensure secure and stable Internet communications, it is essential that Internet users have confidence that they are communicating with the parties with whom they intend. For the Internet to complete its evolution into the key platform for all types of communications, there must be confidence that the global network infrastructure is secure and reliable. Users must continue to be able to trust that they are communicating with the people they intend to communicate with, that they are doing so in a timely fashion, and that the data, video, or voice calls they are sending or receiving remain confidential and their integrity is protected.

An essential element in assuring this security is that domain names have a trustworthy mapping to IP addresses and are not tampered with or disrupted. DNSSEC authenticates communications through the use of *public keys* bound to a unique user to ensure that IP addressing is authentic and accurate. It should be integrated into the Internet to provide for assured distribution of IP addresses and autonomous system numbers. DNSSEC would validate DNS addresses and deter spoofing of Web sites (thereby allowing communications to be misdirected) and other Internet services. Signing the Internet's root zone files (the Internet Assigned Numbers Authority [IANA] root) and the roots for the Top Level Domains (TLDs) would also improve Internet integrity.

4. **Routing Security (Border Gateway Protocol [BGP]; Router Upgrades).** As noted in the discussion of Internet growth, the increase in Internet traffic raises questions of whether computational capacity on root zone servers can meet demand, and whether the constant updating of routing tables will strain the routers' computational ability. The BGP is used to perform interdomain routing on the Internet and is vulnerable to spoofing and misconfiguration, which can lead to the misrouting of Internet traffic. While technologies to increase BGP security, such as Secure BGP and Secure Origin BGP, exist to protect against BGP vulnerabilities, they are expensive, require widespread implementation, and have not been widely adopted by the community. Ultimately, operators will have to step up to the cost or figure out an alternative that eliminates the problem.
5. **Out-of-Band Control Space for the Internet.** The PSTN relies on a parallel, out-of-band network (the SS7 network), to separate telecommunications content from operational control messages. This parallel, out-of-band management approach vastly increases the security and reliability of the PSTN network. Current Internet architecture does not permit out-of-band management of the Internet control space where both communications content and message control information are sent over the same network at the same time. This subjects Internet traffic flow to the risk of tampering and corruption. An out-of-band control space for the Internet could greatly improve the ability to isolate network management data and increase reliability.

Each of these issues has already drawn USG attention. USG reliance on the Internet, or on other agencies and businesses that rely upon the Internet, make the Internet a target for any opponent. The fact that a few highly qualified individuals can create significant trouble in this environment merely underscores the attractiveness of targeting the Internet as a tool of asymmetric warfare in which terrorists as well as nation states can engage.

Organizations

The third trend, changes in how the Internet is governed, simply complicates how to deal with the first two trends.

- The U.S. has had considerable influence over how the Internet has been governed, but that influence is now likely to wane for several reasons. First, as the Internet becomes more embedded around the world, the technical expertise that once resided largely, if not exclusively, in the United States is becoming dispersed. Second, the creators of the Internet, many of whom were once employed by the USG and who, through its prestige, history, and expertise continue to have considerable influence in the various governance forums, are now retiring. Third, virtually all governments now recognize the importance of the Internet for economic reasons, and there is universal appreciation of the Internet's capability to enhance free speech – a positive value to many nations but a threat to others. For one reason or another (or both), some governments now want to control Internet decision-making. They seek to displace the private sector, which has largely had control over key Internet-related decisions for the past two decades as a result of U.S. policy in favor of such control. Similarly, some want to displace the role of the United States, which maintains some limited control by its agreements with the Internet Corporation for Assigned Names and Numbers (ICANN) and the IANA, both of which play a role in the domain name system that assigns Internet addresses and authorizes TLDs (such as .com).
- The American private sector, on which the USG has relied to represent its interests because of their close alignment on most significant Internet policy questions, is growing increasingly globalized. The close working relationship may not be sustainable in that environment.

> *"IANA would be the logical holder of the public part of the signed root key, but its connection with the USG raises serious objections in some quarters from those who claim to fear that the USG could use its influence to disrupt traffic to and from countries it opposes."*

The responses to these challenges are both short- and long-term:

1. **Resolving the Status of ICANN.** The USG, through the Department of Commerce (DoC), created ICANN in 1998 and contracted with it to operate IANA, which performs vital IP addressing functions, including maintaining the domain addresses on the Internet's 13 root zone servers (and more than 100 anycast clones). Since then, the DoC has maintained a Memorandum of Understanding (now a Joint Project Agreement [JPA]) with ICANN, the purpose of which is to ensure that ICANN would become sufficiently democratic, transparent, accountable, and efficient so that it could be allowed to fully privatize. The current JPA ends in 2009, and the DoC has received comments in response to a Notice of Inquiry as a mid-term review regarding ICANN's status in becoming secure and stable organization.[8] The problem is complex: not only is there the issue of whether ICANN has met its goals, but also there is the problem of whether a fully privatized structure can be guaranteed protection from other governments' attempts to exercise unwanted influence over its operations. Although there is no equivalent issue with regard to IANA, with which the USG has not promised to eventually terminate its contract, other governments contin-

ue to press for a change in IANA's status. The dispute has other ramifications. IANA would be the logical holder of the public part of the signed root key, but its connection with the USG raises serious objections in some quarters from those who claim to fear that the USG could use its influence to disrupt traffic to and from countries it opposes.

2. **Defining the Role of the International Telecommunication Union (ITU).** The ITU is a United Nations-related agency that, for many decades, has been the principal international forum for standards related to telephone service.[9] It is also the only significant organization related to Internet governance where governments are the sole voting parties. The ITU has long played a role with regard to the Internet. Because the Internet is carried over telephone networks, standards related to those networks' involvement in the Internet are often addressed by the ITU. However, some governments see the ITU as a way to extend their influence over Internet decision-making and, therefore, are pressing for an expansion of the ITU's role in Internet-related issues. The ITU's leadership seems open to some of these ideas. The Secretary General of the ITU recently told a gathering in Washington, D.C., that he would consider having ICANN's government advisory committee become a function of the ITU. Some of those questions are likely to be addressed during the World Telecommunications Standards Assembly, to be held later this year, and the World Telecommunications Policy Forum scheduled for 2009.
3. **Artificial Intelligence as a Substitute for Organizational Control.** Those who control the technical hierarchies and centralized nodes of the Internet also hold greatest power over the network and, ultimately, its users. There needs to be research to explore the possible reconfiguration of the DNS protocols and any other infrastructure tools that are inherently hierarchical or centralized in nature with a view toward eliminating as many technical points as possible that require human decision-making. Research should also be conducted to determine whether changes in protocols and use of artificial intelligence at key decision points, together with increased use of mirroring, open architectures, and other transparencies would enable greater overall system adjustments via competitive market forces rather than through organizations, such as ICANN, which would reduce the pressure for increased political control.

The Way Forward

The way forward must focus on research and representation. There are a variety of defense organizations that fund projects that address the evolutionary aspects of Internet R&D or alternative technologies, including the Army, the Naval Research Labs, and DARPA. DARPA recently released a Request for Information for Assurable Global Networking, suggesting a renewed interest from DARPA in alternate technologies. Part of their work involves participating in the White House's Office of Science and Technology Policy's Networking and Information Technology Research and Development program, which is the result of the High-Performance Computing Act of 1991, 105 Stat. 1594, and the Next Generation Research Act of 1998, 112 Stat. 219.[10]

The challenge for the DoD is assuring the continued coordination of all this work to ensure security and stability within the fast-changing Internet and the increasing capabilities of those attacking its security and stability. The needs of the GIG are driving some of this activity, as are the tactical and strategic concerns surrounding terrorist and nation-state use of the Internet against our national security interests. The National Defense University will shortly publish an extensive report on *cyber power* that may help facilitate the discussion, but developments happen so quickly that the discussion must be constant and intense. The evolving recognition of the significance of the challenge and its broader implications for national security should push current activity to an even higher level.

Similarly, the DoD currently participates in some organizations that are involved in Internet-related decision-making. As the operator of .mil, the DoD tracks activity in the American Registry for Internet Numbers, the Regional Internet Registry for North America, and parts of the Caribbean. The DoD also monitors developments in the Internet Engineering Task Force (IETF), which sets standards for core

Internet functions, and the related Internet society. The DoD has regularly been active at the ITU, although with a greater focus on the wireless spectrum rather than the Internet. In many cases, the DoD has only had the ability to monitor developments, and not to drive activity or offer leadership in these organizations that are reputation-based and require active and sustained participation.

The continuing challenge is to coordinate all of these activities within the DoD, with the rest of the USG, and with the American private sector. The ability to influence cannot rest solely on one's government status. Even at the ITU, where governments control the votes, key policy decisions about telephone networks are made in the study groups where the private sector dominates. Influence there is dependent on constant and highly competent participation by individuals. The same is true at ICANN and the IETF. Hence, the DoD's ability to analyze issues based on its vast technical insights, its needs as a user, and its status as an Internet service provider give it a unique ability to work in these environments. Other agencies have important roles to play, but their work can be powerfully enhanced by committed DoD support.◆

Reference

1. Wired.com. "Bush Administration Restates Position on Proposed Internet Traffic Policing Rules." Wired.com. Sept. 2007 <http://blog.wired.com/27bstroke6/2007/09/bush-administra.html>.

Notes

1. A megacommunity is defined and referenced as the following:

> ... a public sphere in which organizations and people deliberately join together around a compelling issue of mutual importance, following a set of practices and principles that will make it easier for them to achieve results. Like a business environment, a megacommunity contains organizations that sometimes compete and sometimes collaborate. But a ... megacommunity is a larger ongoing sphere of interest, where governments, corporations, non-governmental organizations, and others intersect over time. The participants remain interdependent because their common interest compels them to work together, even though they might not see or describe their mutual problem or situation in the same way.

Booz Allen Hamilton. The Megacommunity Way: Mastering Dynamic Challenges With Cross-Boundary Leadership. July 2007 <www.boozallen.com/publications/article/38632762>.

2. FCC Notice of Inquiry. In the Matter of Broadband Industry Practices. WC Docket No. 07-52, adopted 22 Mar. 2007.
3. Office of Management and Budget. "Memorandum for Chief Information Officers." Transition Planning for Internet Protocol Version 6 (IPv6). 2 Aug. 2005 <www.whitehouse.gov/omb/memoranda/fy2005/m-05.22.pdf>.
4. Lucky, Robert, and Jon Eisenberg, eds. Renewing U.S. Telecommunications Research. National Academies Press, 2006.
5. See <www.geni.net>.
6. For a further explanation of this concept, see Tim O'Reilly's Web site <www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/what-is-web20.html>.
7. Traynor, Ian. "Russia Accused of Unleashing Cyberwar." The Guardian 17 May 2007 <www.guardian.co.uk/world/2007/may17/topstories3.russia>.
8. NTIA. "Statement of the Mid-Term Review of the Joint Project Agreement (JPA) Between NTIA and ICANN." 1 Apr. 2008.
9. See <www.itu.int>.
10. See 15 USC Sec. 5501 et. seq. for the text in the U.S. Code.

Additional Reading

1. Loren Data Corp. "A Military Networking Technology for Global Information Exchange." FedBizOpps 13 Sept. 2007 <www.fbodaily.com>.
2. Hayes, Frank. "Frankly Speaking: Pakistan's BGP Sabotage Bodes Ill for IT." Computerworld 3 Mar. 2008 <www.computerworld.com>.
3. Karlin, Josh, Stephanie Forrest, and Jennifer Rexford. Pretty Good BGP: Improving BGP By Cautiously Adopting Routes. University of New Mexico Technical Report TR-CS-2006-10, June 2006 <www.cs.princeton.edu/~jrex/papers/pgbgp.pdf>.
4. Agence France-Press. "Estonia Urges Firm EU, NATO Response to New Form of Warfare: Cyber-Attacks." The RawStory.com. 15 May 2007 <http://rawstory.com/news/afp/Estonia_urges_firm_EU_NATO_response_05152007.html>.
5. Gross, Grant. "ICANN Looks Toward End of U.S. Agreement." IDG News Services 7 Mar. 2008 <www.infoworld.com/article/08/03/07/ICANN-looks-toward-end-of-US-agreement_1.html>.

About the Author

Mitchell Komaroff leads and is the Acting Director of the Globalization Task Force (GTF), for the ASD(NII)/DoD CIO. The GTF is an office within the Office of the DoD CIO dedicated to strategic national security planning to address risks arising from the globalization of the telecommunications infrastructure and of the marketplace for information and communications technology. He is primarily responsible for developing and implementing a strategy for mitigating national security risks to DoD arising from the increasing globalization of the ICT sector. The GTF is the ASD (NII)/DoD CIO focal point for transactional risk management in Committee on Foreign Investment in the U.S. and FCC licensing matters, developing strategies for preserving and improving Internet security and stability in support of DoD and USG communications, and policy development addressing global supply chain risk. Komaroff has worked to implement software and systems assurance across the DoD. He has worked previously as a computer scientist with DISA, and with industry where he worked network quality of service, IA architecture, and information management issues. Komaroff holds a master's degree in mathematics from George Mason University and a Juris Doctor degree from the University of Maryland, School of Law.

Phone: (703) 697-3314
E-mail: mitchell.komaroff@osd.mil

The Unified Cross Domain Management Office: Bridging Security Domains and Cultures

Marianne Bailey
OASD(ILA)

The Unified Cross Domain (CD) Management Office (UCDMO) was established July 2006 to address the needs of the DoD and the IC to share information and bridge disparate networks. Information sharing is a requirement that spans both departments and requires the ability to share information from the most highly classified networks to the most open coalition networks. The UCDMO was created to address the duplication, inefficiencies and resulting ineffectiveness resulting from years of uncoordinated activities in the CD arena.

The UCDMO was established on July 10, 2006, by the Assistant Secretary of Defense for Networks and Information Integration and Department of Defense Chief Information Officer (ASD(NII)/ DoD CIO), the Honorable John Grimes, and the Associate Director of National Intelligence and CIO, the Honorable Dale Meyerrose (ADNI & CIO). As the necessity to share information between the DoD, the IC, and U.S. foreign allies has continuously increased, the ability to bridge disparate networks (security domains) has become critical. Information sharing is a requirement that spans both departments and requires the ability to share information from the most highly classified networks to the most open coalition networks. In the past, these bridges or CD mechanisms were developed behind the doors of each organization for their specific applications. The result from years of doing business in this way has led to many CD stovepipes with independent sustainment tails, a tremendous number of interconnections, inconsistent security and risk-mitigation practices, and inadequate policies.

In addition, customers looking for a solution to enable them to share information across security domains had nowhere to go to seek help and often would develop another stovepiped solution. In the DoD, this flood of components into the current certification process resulted in a wait time anywhere from one to two years before approval to operate was granted. In the IC, there was less consistency among the agencies resulting in varying security practices. In an arena wrought with a lack of standards and excessive duplication, the worst part was that even for those who endured a two-year wait the customer's requirement for sharing information was not being met. In short, the lack of adequate CD mechanisms and common standards, policies and processes were significantly impacting the ability of the United States to ensure critical information was available when and where it was needed. The CIOs realized the need to join forces to solve the CD problem and created the UCDMO to address the duplication, inefficiencies and ineffectiveness resulting from years of uncoordinated activities in the CD arena.

The UCDMO faced two initial challenges: staffing the office, and tackling the initial tasking given to them by the CIOs to clean up the state of CD in the DoD and IC. Specifically, they were charged with getting the list of current operational mechanisms down to 24 specific mechanisms. Meyerrose and Grimes felt that 24 was a reasonable number of discrete CD mechanisms for the community. They wanted to make sure there were enough to fill the requirements of the DoD and IC, but not so many as to cause significant redundancy. With a staff of five, the UCDMO knew they would have to draw upon the community to tackle this task. To obtain support for both the staffing and the initial task, the UCDMO leadership began a series of meetings with all major agency CIOs to request full-time staff as well as participation in all tiger team[1] initiatives.

To address the current state of CD, the UCDMO led a community tiger team to determine a process for vetting the current operational solutions and eventually develop a CD baseline. The team quickly realized the need for a common CD taxonomy to ensure that all communities would speak the same language. First on the list was defining CD. The following definition was developed, vetted through the DoD and IC, and approved:

> A CD mechanism is defined as a form of controlled interface that provides the ability to manually and/or automatically access and/ or transfer information between differing security domains. [1]

The CD taxonomy was released in January 2007 and can be found on the UCDMO Web site[1]. Beginning with an initial list of more than 800 items believed to be CD products, the tiger team developed a fairly simple set of criteria and over the course of three months whittled the list of acceptable CD solutions down to 15 discrete items.

Products on the baseline are determined to meet the community standards and are available for reuse as a point solution or as an enterprise service. Each of these products is approved for a specific implementation such as bridging a top secret to secret domain or bridging a secret to unclassified domain. To make the list more useful to the customer, the UCDMO categorized CD mechanisms as *transfer*, *access*, and *multilevel*. A *transfer* device permits the movement of data from one domain to another. An *access* device allows a user to sit on one workstation and access multiple domains but not move data between them. A *multilevel* device stores and processes information of different security levels in a common repository but only allows a user to view appropriate information based on his/her credentials. CD baseline mechanisms are identified based on these three categories. An updated version of the list is released whenever there is a change to the baseline. The UCDMO Web site[2] contains the latest version of the CD baseline (see Table 1, next page) with descriptions and points of contact for each mechanism. Those items that did not make the baseline were placed in other categories such as research, development, legacy devices, or CD tools and were put into a queue to be handled by a follow-on UCDMO effort. New products are added to the baseline if they meet the following three criteria:

- **Capability.** Address a capability gap or extend current capabilities in a significant manner or lower cost.
- **Certification.** Complete certification testing with no findings of concern.
- **Lifecycle.** Lifecycle support and sustainment for at least three years.

By September 2007, UCDMO staff had grown to 30 individuals. The UCDMO management re-addressed their charter and goals and established four key initiatives to bring the communities together and solve the CD problem:

1. Strategic outreach and communication.

CD Baseline versus 2.1 (Released July 2007)		
Transfer	**Access**	**Multi-Level**
DSG 2.1	HP NetTop 1.3	ML Chat 1.0
DTW 3.4/3.4 N5	DTW 3.4/3.5 N5	TNE 9.0.1
ISSE 3.5B2	Janus 5.1	
MDDS 3.1	MDDS 3.1	
Radiant Mercury 4.0.5 P3	MLTC 3.0	
Smart.neXt 3.0	Secure Office Thin Client v1.1	
TDX 2.3		
TGS 2.1 P1		
TSABI OWT		

Table 1: *CD Baseline*

CD Capabilities	
Push Data	Subscribe/Distribute Information Feeds
	Post Data to Repositories
	Delivery to Specified Recipients
	Import Data
	Export Data
	Transfer Streaming Data
	Perform CD I&A and Attribute Management
Collaboration	Exchange E-mail
	Single Electronic Inbox
	Conduct Instant Messaging and Text Chat
	Shared Workspaces
	Audio Conferencing
	Video Conferencing
Centralized IT Management	Centralized IT Services (DNS, DHCP)
	Centralized Backup and Restore
	CD-Required Capabilities
	Centralized CD Audit
	Centralized Monitoring
	Remote CDS Administration
	Remote IT Administration
	Error Notification
Content Inspection and Release	Enforce Reliable Human Review
	Malicious Content Prevention
	Perform Attribute-Based Access Control
	Hidden Content Identification
	Enforce Content Policy
	Allow Policy Override
	Rules Management
Remote Access Centralized Repository and Other	Application Sharing
	Multilevel Data Repositories
	Network Reduction
	Desktop Reduction

Table 2: *CD Capabilities*

2. Transition to baseline and enterprise services.
3. Align DoD/IC policies and processes.
4. Manage a CD investment strategy.

These initiatives were developed to complement one another as well as address the lack of a single DoD/IC point of contact for CD activities, the disparate and inefficient policies and process, the duplication in research, development and testing, the excessive costs and security risk of managing point CD solutions, and the lack of a focused effort to meet the community's requirements.

The main focus of Initiative 1 is to provide one voice to all organizations involved in the CD space, whether it be customers, policy makers, or vendors. As part of the outreach element, the UCDMO leadership visits the combatant commanders, services, and agencies to provide information and solicit feedback on their recent initiatives and their long-term strategy. The UCDMO holds three types of official forums: customer, developer, and a yearly conference. The customer forum is held on a periodic basis to roll out major deliverables. The October 2007 customer forum was held at the Army Research Lab in Adelphi, Maryland, and was attended by approximately 250 individuals. The forum involved three days of interactive sessions describing the new implementation process and the associated DNI/DoD C&A transformation.

In November, the UCDMO held its first developer forum, known as Developer Days, to begin parsing through all CD research programs. In these sessions, a CD R&D program office provides CD program reviews to a community SME panel. During these reviews, the vendor and their associated government sponsor spend one hour providing information specific to their program, such as CD requirements being addressed, program milestones, status, funding profiles, and program risks. The UCDMO held successive Developer Days in February, March, and April. The recommendations from the SME panel will feed into the CD investment strategy discussed in Initiative 2. Additionally, the UCDMO will hold a yearly CD conference. The first conference was held in May 2007 in San Diego, California. More than 600 customers and developers attended the conference. The Honorable John J. Grimes, the Honorable Dale Meyerrose, and Vice Admiral Brown, JSJ6, were among the keynote speakers. This year's conference is being planned for October 2008. Information will be posted to the UCDMO Web site.

Initiative 2 will ensure that the community moves from legacy point CD solutions to available baseline or enterprise CD services. Every CD connection introduces a risk to the networks and the data. CD solutions are complex and require lifecycle support such as installing security patches and updating malicious code software inspection mechanisms. Since the health of the CD mechanism is so critical to ensuring the security of the device, it is imperative that these devices be rigorously maintained. In the operational world, experience has shown that these devices are not being adequately maintained. The customer does not want the responsibility of deploying and maintaining the CD mechanism; what they want is the capability to share information across domains. Establishing CD enterprise services will solve this issue. Initial CD implementations at the enterprise will provide current CD baseline products in an enterprise capacity. To begin this transition, the UCDMO and enterprise service providers will partner with the customer to roll out CD enterprise services for customers requiring new or replacing legacy CD capabilities. In the DoD, Teresa White leads the DoD CD Enterprise service organization, and for the IC, Dan Nichols at Defense Information Agency is standing up CD services at regional service centers. The focus towards CD enterprise services provides users the required information sharing capabilities without the headaches of acquiring, certifying, accrediting and maintaining point CD mechanisms. Additionally, enterprise CD services will be the avenue for achieving global awareness of enterprise connectivity and greatly improve the security of our networks.

Initiative 3 is critical in ensuring common implementations throughout the community. The UCDMO is linked into the new DNI-led DoD/IC C&A transformation. One of the initial tasks was to develop a common set of security controls that will be recognized and accepted throughout both communities. This is the cornerstone to reciprocity in implementation, reusability, and efficiency. Additionally, the UCDMO has drafted a single CD implementation process that will eliminate the need for duplicative testing, promote sharing bodies of evidence, and provide accelerated approval for CD enterprise or baseline solutions. Both the security controls and the implementation process are available on the UCDMO Web site. The UCDMO is currently developing a series of CD profiles which will identify the minimum security controls required for a transfer, access, or multilevel mechanism. These profiles will assist the development organizations and can be used by vendors as build-to guidance as well as aid the testing organizations in ensuring a common and thorough set of standards. Implementing a common set of policies and procedures across these communities is more of a cultural challenge than a technical challenge. In the past, each community had separate standards and policies in addition to individual accreditation authorities. This may have made sense before our networks were so interconnected, but we must realize that every interconnection, every implementation of a CD solution puts our networks at risk. Many of the current connections were made based solely on mission need without sufficient consideration for protecting the networks and data. There is no arguing that success in moving to a centralized approach for implementing approved CD solutions will require a major cultural change. As the CIOs for the DoD and IC, John Grimes and Dale Meyerrose are committed to ensuring adequate protection of DoD and IC networks and are the catalyst for this change.

The 4th UCDMO initiative is developing a community-wide CD investment strategy. This initiative began almost immediately upon establishment of the UCDMO by consolidating the community CD requirements into a comprehensive list of 31 CD capabilities (Table 2).

Additionally, the UCDMO began to compile a list of all CD R&D efforts throughout the DoD and IC. Today, there is tremendous duplication among these efforts. Most of these programs are targeting the same five or six requirements. There is no coordination or even centralized tracking. It is very difficult for a customer to determine what other similar activities are occurring in the community. The UCDMO mapped the 31 capabilities to the currently available baseline mechanisms and to the known R&D activities resulting in a CD gap analysis. The UCDMO released Version 1.0 of the CD investment summary in March 2008. Additionally, they will provide CD investment recommendations to the CIOs. Some programs will be recommended for termination, others recommended for consolidation, and new programs will be suggested to target CD requirements gaps. The goal of Initiative 4 is to provide a focused, intentional, and targeted CD R&D program.

The UCDMO will also deliver an overall CD strategy for both the DoD and the IC in the CD Roadmap. Building on all four initiatives, this plan will lay the framework to ensure that CD will support both current and future information sharing.

CD is a critical enabler for implementing the President's National Security Strategy goal of information sharing[2]. The work of the UCDMO, coupled with support from the community, will make great strides in reaching that goal. Since its inception, the UCDMO has produced a CD baseline of products available for reuse, a list of known CD mechanisms in R&D, and a list of products that will need to be replaced in the next few years. In addition, a common DoD and IC process for CD implementation has been developed. The UCDMO has also made significant contributions to policies throughout the DoD and IC and will continue to have influence in the future. Success of the UCDMO requires a cultural change in which all partners work toward a common goal of enhancing our information sharing capabilities by fully supporting the UCDMO initiatives.◆

Reference

1. UCDMO. "Committee for National Security Systems Instruction 4009: National Information Assurance Glossary (CNSSI4009)."

Notes

1. A *tiger team* is a group of experts assembled for a set time to accomplish a specific task.
2. <www.intelink.gov/mypage/ucdmo>.
3. <www.whitehouse.gov/nsc/nss.html>.

About the Author

Marianne Bailey is the director of the UCDMO. She has been an employee of the federal government for 23 years and has recently finished a three-year leadership development program while holding positions in DISA and various other federal government organizations. Bailey has extensive IA experience and has provided IA guidance to a multitude of customers from the DoD, IC, and federal government sectors.

UCDMO
Phone: (240) 373-0796
Fax: (240) 373-0807
E-mail: ucdmo_outreach@nsa.gov

DoD Global Information Grid Mission Assurance

Anthony Bargar
OASD/NII, DASD(IIA)

The DoD's policy, planning, and warfighting capabilities are heavily dependent on the IT foundation provided by the GIG. However, the GIG was built for business efficiency instead of mission assurance against sophisticated adversaries who have demonstrated intent and proven their ability to use cyber as a tool for espionage and the criminal theft of data. GIG mission assurance works to ensure the DoD is able to accomplish its critical missions when networks, services, or information are unavailable, degraded, or distrusted. This article explores current threats to the GIG and outlines the solutions that the DoD has developed to protect our networks.

The information environment in which the DoD operates is global, mobile, and interconnected. Dependence on shared critical information infrastructures are a strategic advantage as well as a weakness. National security is challenged by sophisticated adversaries who have demonstrated intent and proven their ability to use cyber as a tool for espionage and the criminal theft of data. Successfully defending the DoD's networks and information from sophisticated adversaries is a serious challenge. Unlike the hacker community, sophisticated adversaries are well resourced, trained, and often have the backing of foreign intelligence services, transnational groups, or organized crime. Sophisticated adversaries leverage a full range of information operations to achieve their goals. Every year, attempts to penetrate DoD networks increase; still, there has been no wide-scale disruption of the critical information infrastructures on which the DoD depends for mission success.

However, in February 2008, the IC warned of increasing cyber attacks by foreign governments, non-state actors, and criminal elements exploiting vulnerabilities of the U.S. information infrastructure [1]. Sophisticated adversaries have the technical means, the insider knowledge of national infrastructures, and the intent to manipulate data and disrupt critical and vulnerable national resources. At the same time, the DoD Inspector General published an audit of the DoD's mission-critical IT systems which found that 61 percent lacked contingency plans or evidence of such plans, and 82 percent have never been exercised, leading the audit to conclude that " ... DoD mission-critical systems may not be able to sustain warfighter operations during a disruptive or catastrophic event" [2].

National security depends on assured global information infrastructures that are reliable and resilient. Real-time risk management and situational awareness are essential to responding to a cyber crisis, as is the consideration of what national security missions are affected, potential cascade effects, and the prioritized approaches for restoration.

> **"National security depends on assured global information infrastructures that are reliable and resilient. Real-time risk management and situational awareness are essential to responding to a cyber crisis ..."**

The DoD's policy, planning, and warfighting capabilities are heavily dependent on the IT foundation provided by the GIG. Net-centric information environments provide reliable, instant, and meaningful information that shape DoD positions, as well as prepare and enable a joint warfighting force to dominate air, land, maritime, and space. In 2006, the DoD aligned cyberspace as a warfighting domain alongside the traditional domains of air, land, maritime, and space. However, it is not a sanctuary advantage for the DoD, but a borderless, pervasive, and hostile operating environment for all missions.

In February 2007, responding to growing threats to the GIG, the DoD took additional steps to increase resilience against sophisticated cyber attacks. DoD leadership recognized that the solution set included a broad spectrum of experts from IA, the Homeland Security Critical Infrastructure, and the Joint Chiefs of Staff. A working group was charged with analyzing the issue and laying out a plan of action to ensure that the DoD is able to accomplish its critical missions when networks, services, or information are unavailable, degraded, or untrusted. The DoD's mission-essential functions (MEFs) such as deploying the armed forces, maintaining command authority, and global situational awareness were deemed critical. GIG mission assurance was defined as *the level of confidence that the GIG will provide adequate support for critical MEFs in the face of full-spectrum attack from a sophisticated adversary*.

The scope of the problem includes the networks, services, and information needed to conduct cyberspace operations, consistent with the National Military Strategy for Cyberspace Operations and other documents such as the National Strategy to Secure Cyberspace [3] and the National Response Framework [4]. Additionally, to improve resiliency, protection, and continuity of services, the underlying infrastructures such as power and telecommunications networks are critical to the DoD's ability to conduct its missions. Guiding principals for the initiative include the following:

- GIG mission assurance is a continuously changing and adapting set of capabilities protecting against all adversaries which ensures execution of mission essential functions.
- GIG mission assurance is built on survivable communications (transport),

trustable information (content), and timely services (applications).

- Mission operations (the warfighter) must allow for and compensate for failures and losses from natural and human adversaries that are persistently present.
- The GIG must provide force-wide survivable, robust, and resilient capabilities against sophisticated adversaries.

The problem domain is large and spans people, processes, technology, associated training, policy/governance, and architectures. There are many disciplines and organizations involved within the DoD including, but not limited to, cyber protection, detection, reconstitution, intelligence, continuity of operations, and critical infrastructure protection. Additionally, the DoD's role in national response, emergency preparedness, and support must be considered in a holistic approach for addressing how the GIG enables essential missions. Ensuring the DoD can accomplish these missions while operating in a degraded information environment requires a much broader range of activities, and requires close coordination between the IT community and the warfighter. For example, to accomplish the MEFs, the warfighter must define more concise technology requirements as well as train and equip forces to achieve mission success despite a degraded cyber domain. Additionally, the IT community must provide the warfighter situational awareness for failure and cascade effects of the GIG as related to specific MEFs, and build diverse and resilient capabilities. During a sophisticated attack, the IT community must restore capabilities to support current mission priorities as the warfighter compensates for loss in services. In short, the DoD's response activities must operate at *the speed of light, verses the speed of policy*. Response options must be synchronized, prioritized, and coordinated to minimize effects on national security missions and ensure that MEFs can successfully survive an attack.

Conclusion and 2008 Priorities

In a net-centric information environment that is globally interconnected, there are insufficient resources to protect and defend all aspects of the GIG at all times from growing and asymmetric threats. Additionally, the DoD GIG can be denied or degraded by non-cyber events on dependent critical infrastructures such as power and telecommunications. A change in philosophy is needed, as well as an integrating framework for a holistic approach balancing resources and risk to protect our capabilities which enable MEFs. There are steps both strategic and actionable to improve the DoD's posture and ability to survive sophisticated cyberspace attacks. GIG support to mission assurance requires integrated plans, programs, and operations across IA, computer network defense, cyberspace intelligence activities, and critical infrastructure protection. To better understand the shortfalls and enable solutions, DoD priorities in this area include the following:

- Exercising military operations under a severely degraded cyber environment.
- Improving resilience, prioritization for recovery, and continuity of operations.
- Redefining network command and control capabilities with regard to prioritized reconstitution of GIG services.
- Resourcing and planning for mission assurance with combatant commands, services, and agencies.

> *"The bottom line is that the GIG is DoD's force multiplier for mission success in air, land, sea, and cyberspace ...The DoD is acting on the solutions necessary to ensure mission success."*

The bottom line is that the GIG is the DoD's force multiplier for mission success in air, land, sea, and cyberspace. The GIG must compensate for loss due to cyberspace disruption, and the users must prepare to operate in a degraded environment. The DoD is acting on the solutions necessary to ensure mission success.◆

References

1. "Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence." 5 Feb. 2008 <www.dni.gov/testimonies/20080205_transcript.pdf>.
2. Office of the Deputy Inspector General. "Contingency Planning for DoD Mission-Critical Information Systems." 5 Feb. 2008 <www.dodig.osd.mil/Audit/reports/fy08/08-047.pdf>.
3. "National Strategy to Secure Cyberspace." Feb. 2003 <www.whitehouse.gov/pcipb>.
4. Department of Homeland Security. "National Response Framework." Jan. 2008 <www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.

About the Author

Anthony Bargar is a senior policy analyst leading DoD's GIG mission assurance for the DASD(IIA) where he leads the strategic goal to transform and enable IA capabilities for the DoD and supports the DoD's IA responsibilities in the interagency critical infrastructure protection programs. Previously, he served as IA-Senior Technology Advisor for the Counterintelligence Field Activity, and Senior IA Analyst for the Defense Intelligence Agency, where he implemented the Defense Intelligence Communities Enterprise Risk Management System. Bargar led a research project for the DoD on shared critical information infrastructure protection and defense with the National Defense University (NDU) and the Swedish National Defense College. He holds a master's degree in information and telecommunication systems for business from Johns Hopkins University. Additionally, he is a distinguished graduate from the NDU Information Resources Management College.

E-mail: anthony.bargar@osd.mil

Educated and Trained Information Assurance Workforce: Key to Our Mission Success

George Bieber
Director, Information Assurance Workforce Improvement Program

The article summarizes the DoD's strategic IA workforce objectives, progress made in 2007 toward implementation, and the way ahead in 2008 and beyond.

Just like any organized structure, a highly networked systems environment is only as good as its people. Federal agencies and organizations are unable to protect the integrity, confidentiality, and availability of information without a workforce that is adequately trained and educated in IA. DoDD 8570.1, *IA Training, Certification, and Workforce Management*, and its accompanying IA Workforce Improvement Program (WIP) manual (DoD 8570.01-M), represent the first steps toward building and making professional the IA workforce within the DoD.[1]

The IA WIP implements the requirements of DoDD 8570.1 and establishes the organization's IA WIP policy and procedures. Its initiatives are aligned to the DoD Information Management/IT Strategic Plan. The program's vision is to establish an IA professional workforce with knowledge, skills and abilities to effectively prevent, deter, and respond to threats against DoD information, information systems, and information infrastructures. Integral to this vision is the ability to effectively manage the IA workforce to place people with the right skills in the right place at the right time.

The foundation to build this capability consists of the following five strategic IA workforce objectives:

1. **Certify the workforce.** Establish baseline certifications across the enterprise and certify the workforce according to those baselines.
2. **Manage the workforce.** Provide the tools to facilitate both component management of its IA workforce and the insight of the OSD into DoD's overall workforce status and certification posture.
3. **Sustain the workforce.** Enable DoD workforce to receive continuous learning opportunities to keep their skills current to combat new network threats.
4. **Extend the discipline.** Infuse IA into professional education programs to expand operational leadership's attention to the domain.
5. **Evaluate the workforce.** Establish a means of assessing compliance and measuring program effectiveness.

Milestones to Success

The 2007 calendar year marked the conclusion of the first year of a four-year implementation plan for the IA WIP. Significant milestones were met throughout the year within each strategic objective area. The following are a few of these important milestones:

- **The DoD met its goal to certify 10 percent of the IA workforce for 2007.** The CIO DIAP, charged with the oversight of the IA WIP, put in place a number of initiatives to assist DoD component IA managers and personnel to achieve this goal including certification self-assessment programs. For example, the International Information Systems Security Certifications Consortium (ISC2) Self Assessment Program for the DoD, provided Certification Information System Security Professional (CISSP) candidates access to practice exam questions that yielded measurable results for students to assess their level of preparedness. Self-assessment programs are also available for students seeking Global Information Assurance Certification, Information Systems Audit and Control Association, and Computing Technology Industry Association certifications.
- **The CIO DIAP put the enterprise-wide concept into practice by developing and conducting a certification voucher program on behalf of the DoD components (known as the Voucher Pilot Program).** Personnel certification requirements were gathered from the components and coordinated with commercial certification providers in the form of bulk voucher purchases. The Personnel Certification Support System (PCSS), an online voucher management system, maintained all voucher allocation and distribution information for each component. The PCSS will continue to be used for the second year of implementation as an effective tool to manage certification vouchers.
- **Upgrades to the Defense Civilian Personnel Data System (DCPDS) are complete and the IA personnel data entry process is under way.** Components must now enter all relevant civilian IA workforce data into the DCPDS including IA positions held and appropriate training and certification requirements. This milestone achievement brings components a step closer to more effective civilian workforce management. Increased workforce management provides leadership with assurance that qualified IA personnel are filling IA positions.
- **The Defense Federal Acquisition Regulation Supplement (DFARS) required by DoD Directive 8570.1 is officially approved and can be used in new solicitations and resulting contracts.** The new clause was published in the January 10, 2008 issue of the Federal Register. The announcement included actual wording for the clause regarding IA contractor training certification. DFARS guidance instructs that any modifications to existing contracts will have to be negotiated with the contractor.[2]
- **DISA-supported enhancements of the Carnegie Mellon University developed Virtual Training Environment (VTE) to provide training to meet DoDD 8570 requirements.** The CIO DIAP has funded specific training and lab capabilities for this program, making it available at no cost to 10 percent of DoD personnel in 2007. The VTE is a resource to DoD employees for information assurance, incident response and computer forensic training, with close to 600 hours of materials available. The environment delivers classroom instruction and self-paced online training for CompTIA security+ and ISC2 CISSP to name a few. Seven DoD 8570.01-M role-based optional courses are currently available for personnel. Additional training courses will be offered in the near future.

- **In fiscal year 2007, 29 students graduated from the program and are currently working full time in IA strategic positions across the DoD. The DoD IA scholarship program awarded 269 scholarships to students seeking bachelor's, master's and doctorate degrees in IA fields of study since the program's inception in 2001.** The DoD IA Scholarship Program (IASP) awarded 269 scholarships. In fiscal year 2007, 29 students graduated. The IASP provides educational incentives to foster the recruitment and retention of qualified IA/IT personnel. As a resource for DoD IA professionals to continuously enhance their skills and to keep current with technology and threats, the IASP supports the IA WIP strategic objective to sustain the workforce.[3]

Monitor Success

As the message about the IA WIP program disseminates across the DoD, the goals become more rigorous and the mission more clear. The second year (2008) of the program's implementation includes the following new challenging milestones:

- By the end of 2008, 40 percent of the DoD workforce must be certified according to DoD 8570.01-M baseline policy requirements.
- New specialty positions were proposed for integration into a second change to the 8570.01-M including C&A and software application developers. SME working groups will be organized to focus on the strategy and planning to execute these proposed changes.
- The strategic IA workforce objective, *Evaluate the Workforce*, will play a greater role in program activities. The first IA WIP site review will be conducted in the first quarter of 2008. The intent of these site reviews is to verify DoD component compliance with requirements of DoDD 8570.1 and 8570.01-M. Furthermore, on-site inspections provide the opportunity for the DIAP to assess the level of effectiveness of the IA WIP at the operational level.

Achieve Success

Ultimately, the DIAP seeks to foster continued improvement throughout each year of the program's lifecycle. The implementation planning strategy of the IA WIP dictates a continuous cycle of milestone achievement, benefits actualization, oversight, and improvement. Adherence to this planning strategy will result in a better trained, certified, and professional DoD IA workforce. Results will yield a more capable workforce – and the more capable the workforce, the more likely it is to achieve DoD mission success.◆

Notes

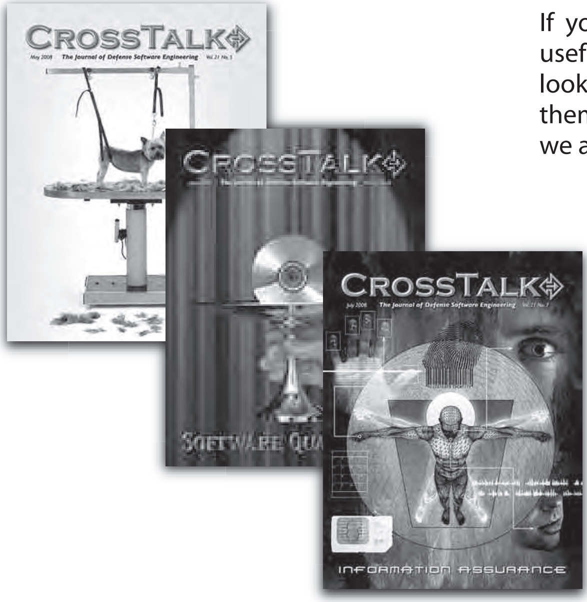
1. Supporting documents can be found at <www.whs.mil>.
2. The full guidance can be found at <www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html>.
3. More information about the IASP can be found at <www.defenselink.mil/cio-nii/iasp>.

About the Author

George Bieber is the Director of the IA WIP program under the DoD CIO. He oversees implementation of the DoD IA WIP, the DoD IASP, and the DoD Shared Service Center for Tier 1 Security Awareness Training under the Office of Management and Budget-mandated Information System Security Line of Business. Bieber served on the President's Critical Infrastructure Protection Board Education Standing Committee, and is a past executive board member of the Federal Information System Security Educators Association. He currently serves on the American National Standards Institute Personnel Certification Accreditation Committee.

Phone: (703) 602-9980
E-mail: george.bieber@osd.mil

CALL FOR ARTICLES



If your experience or research has produced information that could be useful to others, CrossTalk can get the word out. We are specifically looking for articles on software-related topics to supplement upcoming theme issues. Below is the submittal schedule for three areas of emphasis we are looking for:

Software Measurement
February 2009
Submission Deadline: September 12, 2008

Software as a Service
March 2009
Submission Deadline: October 17, 2008

Web-Enabling Applications
April 2009
Submission Deadline: November 14, 2008

Please follow the Author Guidelines for CrossTalk, available on the Internet at <www.stsc.hill.af.mil/crosstalk>. We accept article submissions on software-related topics at any time, along with Letters to the Editor and BackTalk. We also provide a link to each monthly theme, giving greater detail on the types of articles we're looking for at <www.stsc.hill.af.mil/crosstalk/theme.html>.

Transforming IA Certification and Accreditation Across the National Security Community

Eustace D. King
OASD(NII)/DoD CIO

The IA C&A transformation is a partnership that stretches across the DoD, DNI, CNSS, National Institute of Science and Technology (NIST), and the Office of Management and Budget. Much progress has been made since the DoD and DNI CIOs published an initial set of transformation goals in January 2007; however, much work remains. While core transformational documents are being authored through the CNSS and NIST, many of their underlying transformational concepts are being implemented in the DoD through the new DIACAP and in the intelligence community through the near-final IC Directive 503.

The C&A transformation is actually part of a larger transformation. Within the DoD, this transformation is centered on net-centric operations as set forth in the National Military Strategy[1] with the GIG as a critical enabler. Within the IC, it is centered on a drive toward integration, customer service, and advances in analytic capability.

What is common across the DoD and the IC is the need to leverage the power of information through sharing and collaboration. This means ensuring that useful, understandable information is visible and available where it is needed, when it is needed, and to those who need it. It also means that users and entities acting on their behalf (e.g., software services) can connect and partner to generate new knowledge, get work done, or conduct net-enabled operations.

Because the way the national security community creates and uses information is changing, it must change the way it builds networks, provisions services, and manages data. In turn, it must change the way it works together to *identify, validate, authorize, manage, and sustain IA capabilities*, which are the objectives of C&A[2].

Thus, the C&A transformation is about changing the way the national security community manages IA risk. This means breaking down unnecessary barriers between community members and improving information sharing among the security, IT provider, and IT user communities. C&A originated during the days when a few, large standalone mainframes with custom code were typical, and a *steady state* with quantifiable residual risk was expected. The national security community is transforming to service-centric, globally interconnected information enterprises constructed largely from commercially acquired general purpose IT. The legacy, system-centric practice of C&A hinders information sharing and blocks the timely delivery of mission-critical systems.

Table 1: *NSS Documents Currently Under Formal Community Review*

Document	Purpose	Status
CNSSP 22	Establishes a national risk management policy for national security systems.	Under formal review by CNSS
CNSSI 1199	Establishes the way the national security community categorizes information and information systems with regard to confidentiality, integrity, and availability.	Under formal review by CNSS
CNSSI 1253, aka Security Controls Catalog	Consolidates DCID 6/3, DOD Instruction 8500.2, NIST SP 800-53, and other security sources into a single cohesive repository of security controls.	Under formal review by CNSS
CNSSI 1253A	Provides methodology for assessing adequacy of each security control, e.g., testing.	In progress
CNSSI 1260	Provides guidance to organizations with the characterization of their information and information systems.	In progress
Next Generation NIST 800-37	Defines the C&A process (joint DNI, DoD, NIST activity).	In progress

What Is the Status of the C&A Transformation?

While the C&A transformation was initiated by and remains under the joint sponsorship of the DoD and DNI CIOs, key partners include the CNSS, particularly the C&A working group, and the NIST, particularly the computer security division. The engagement and sponsorship of the CNSS allows key policies and guidelines to be developed and published for a broader community: all federal departments and agencies with NSS. Engagement with NIST allows for synchronization of concepts, standards, and guidelines across both NSS and non-NSS. Some of these documents are currently under formal community review in the CNSS; others are still in the drafting stage (Table 1). Other supporting activities, including transition planning and training, are ongoing.

Transition may vary in time and manner across the national security community. Some organizations are planning to follow the C&A transformation process and doctrine even while documents are going through final review. Others may wait until the authoring process is completed, which is expected to occur around the end of calendar year 2008. Readers must look to each department's or agency's policy issuance for these details. For example, the IC's transition details are being promulgated in IC Directive 503 and supporting issuance whereas the DoD's transition details are being promulgated in the DoD 8500 series, primarily the new DoD Instruction (DoDI) 8510.01, the online DIACAP knowledge service[3], and an upcoming revision of DoDI 8500.2.

What Are the C&A Transformation Goals?

In January 2007, the DoD and DNI CIOs published seven goals for transforming C&A processes across the DoD and the IC. The following are the original seven goals along with some implementation details. While the DoD-IC partnership is highlighted, the expectation is that many of the outcomes and benefits described will be realized across the greater national security community and between NSS and non-NSS.

1. **Define a common set of impact levels and adopt and apply them across the DoD and IC.** These are being defined in the new CNSS Instruction (CNSSI) 1199 with consideration for the authorities, complexities, classification needs, and special risks inherent in the national security community.
2. **Adopt reciprocity as the norm, enabling organizations to accept the approvals by others without retesting or reviewing.** Commonly recognized types of national security information and systems are being described in the new CNSSI 1260. These will be supported by reciprocity profiles, tailored sets of security controls for sharing specific types of national security information or systems. Commonly recognized types of information and systems with associated reciprocity profiles will provide agreement on security objectives. Common security controls and assessment methods will provide transparency of security implementation.
3. **Define, document, and adopt common security controls, using NIST SP 800-53 as a baseline.** The new CNSSI 1253 is a comprehensive information system security controls catalog that starts with NIST Strategic Plan 800-53 and normalizes and consolidates the controls from DoDI 8500.2, DCID 6/3, the UCDMO, and CNSS policies (for example, CNSS Policy 12, *National Information Assurance Policy for Space Systems Used to Support National Security Missions*), as well as new controls developed through research related to emerging topics such as outsourcing, supply chain risk, and service-oriented architecture. The new CNSSI 1253A is a companion document that provides common assessment objectives (i.e., expected results) and methods for the common controls.
4. **Adopt a common lexicon, using CNSSI 4009 as a baseline, thereby providing both the DoD and IC a common language and common understanding.** The new CNSSI 4009 will serve as a shared dictionary.
5. **Institute a senior risk executive function, which bases decisions on an enterprise view of risk considering all factors, including mission, IT, budget, and security.** The previous DoD C&A process was intended to balance mission, program, and security risk, but the horizon was local, not enterprise. Today's complex, many-to-many relationships among missions, business functions, and supporting information systems require a holistic, enterprise-wide view to managing risks. The DoD is implementing this goal via the DIACAP governance structure established in DoDI 8510.01. The DIACAP governance structure establishes C&A roles and responsibilities and collaboration mechanisms at every organizational level, from GIG mission areas to heads of components and their chief information officers to individual system program managers, developers, and operators. This comprehensive governance structure is intended to establish a relationship between aggregated information security risks and organizational or enterprise mission and business risks while helping individuals with responsibilities for system implementation and operations to better understand how the information security issues associated with their systems translate into organizational or enterprise security concerns. Over time, the DoD expects to continue to improve this structure and strengthen its interfaces with IC governance structures. Additionally, as part of the next generation 800-37, the DoD is working with NIST and the DNI to address C&A processes for federated enterprises, i.e., for systems and services that span departments and agencies, coalitions, or international strategic partners
6. **Incorporate IA into enterprise architectures and deliver IA as common enterprise services across the DoD and IC.** The DoD is implementing this goal via the IA component of the GIG integrated architecture, a new alignment framework for GIG IA, and a suite of IA capabilities and services being realized though the GIAP.
7. **Enable a common adaptable process that incorporates security within the lifecycle processes and eliminates security-specific processes.** The DoD is implementing this goal via continued integration of IA into the Joint Capabilities Identification and Development System[4].

Who is responsible for coordinating the DoD's participation in the C&A transformation?

- CIO-to-CIO Relations: Gus Guissanie, Principal Deputy, DASD(IIA).
- C&A Operations: Eustace King, DIACAP Program Manager.
- DoD IA Policy: Don Jones, Senior Policy Advisor.

Special Thanks

With input from Sharon Ehlers, Office of the Associate Director of National Intelligence and CIO, and Ron Ross, Computer Security Division, IT Laboratory, NIST.◆

Notes

1. An unclassified version is available at <www.defenselink.mil/news/Mar2005/d20050318nms.pdf>.
2. For example, see the DIACAP definition in DoDI 8510.01, Nov. 2007 <www.dtic.mil/whs/directives/corres/ins1.html>.
3. <https://diacap.iaportal.navy.mil>.
4. Chairman of the Joint Chiefs of Staff Instruction 3170.01F. 1 May 2007 <www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf>; the Defense Acquisition System (DoDD 5000.1), and related issuance, <https://akss.dau.mil/dapc/index.aspx>); and NetOps <www.stsc.hill.af.mil/CrossTalk/2007/07/0707Lam.html>.

About the Author

Eustace D. King is assigned to the Office of the DASD(IIA). As the principle authority within OSD(NII) IAD for ensuring successful implementation of the DIACAP, King provides oversight and community outreach to ensure understanding and adherence to DIACAP policy vis-à-vis DoDI 8500.2, IA implementation. King is also responsible for fielding and ensuring enterprise-wide training for the Enterprise Mission Assurance Support Service, and management of the DIACAP Knowledge Service. He co-chairs the CNSS Sub-Committee, providing leadership to the federal community to aggregately embed IA principles and services within NSS. King retired from the Air Force in 2000.

DASD/IIA-DIAP
Phone: (703) 602-5044
Fax: (703) 602-7209
E-mail: eustace.king@osd.mil

Web Sites

IA Support Environment

http://iase.disa.mil/index2.html

With the banner, "Your one stop shop for IA information," this site is sponsored by the Defense Information Systems Agency, and offers links to a wide variety of IA-related topics including IA training, IA tools, vulnerability management, and important announcements. The subject matters covered include application security, computer network defense, high assurance internet protocol, and CD solutions. There is also a link to upcoming conferences and workshops.

Global IA Certification (GIAC)

www.giac.org

The primary goal of this Web site is to address the need to validate the skills of security professionals and developers. GIAC certification provides assurance that a certified individual meets a minimum level of ability and possesses the skills necessary to do the job. The standards for the GIAC certification were developed using the highest benchmarks in the industry. The site offers a complete breakdown of the GIAC process.

The Center for Education and Research in IA and Security (CERIAS)

www.cerias.purdue.edu

The mission of CERIAS is to advance the knowledge and practice of IA and security through the performance of world-class research, the delivery of the highest quality education, and by serving as an unbiased source of information locally, nationally, and internationally. CERIAS is unique among national centers in its multidisciplinary approach to problems, ranging from purely technical issues (e.g., intrusion detection, network security, etc.) to ethical, legal, educational, communications, linguistic, and economic issues, and the subtle interactions and dependencies among them.

National IA Training and Education Center (NIATEC)

http://niatec.info

NIATEC is a consortium of academic, industry, and government organizations with the goal of improving the literacy, awareness, training, and education standards in IA, and is based at Idaho State University. As the federally designated cornerstone for essential education and training components of a strong IA initiative, NIATEC's mission is to establish an effective IA infrastructure for academic, industry, and government organizations. NIATEC has been active in the development of training standards associated with both the National Institute of Standards Publication 800-16 and the National Security Telecommunications and Information Systems Security Committee 4011, 4012, 4013, 4014, 4015, and 4016 documents.

Engineer's Cadenza in G Minor

Confused about IA? Join the club. Confidentiality, integrity, authentication, and availability dominate the chatter while effective and useful are taciturn in IA circles. Are we talking assurance as in "a declaration to inspire confidence" or assurance as in "that which is designed to give confidence?" I'm hearing a lot of declaration and not much design or confidence. What's an engineer to do?

Sit back, relax, pop in the ear buds, and crank up Johann Sebastian Bach's third movement of the Brandenburg Concerto #3. Listen to the uniform division of parts between the three string groups. Listen how they combine to play in unison and then dart off into a varied musical dialogue. As they glide on separate melodic paths, never does one string dominate or another pale. They never compete or collide, but exist in one accord.

For me, this is what an effective information highway would sound like if it made sound. You can hear streams of information dancing across the wires and airways from destination to destination; frenzied, wispy, vigilant, yet congruent. Bach maintained order, confidence, and integrity in this movement without stifling creativity – a masterpiece in balance. Is that what you hear when you ramp up on the world's wide web of information?

Me neither.

With identity theft, scams, downtime, and data loss it's no wonder there is a push for more confidence, integrity, and availability in computing; much like the Pythagoreans – students of the right triangle theory guy – who wanted to bring order and integrity to music.

Pythagoras of Samos and his followers were musicians as well as mathematicians. Pythagoras wanted to improve the music of his day, which he believed was too hectic. Who knew that Johnny Rotten and Sid Vicious were Greek?

According to legend, Pythagoras thought the sounds emanating from local blacksmith's anvils were beautiful and harmonious. Can't you see Pags in jeans and t-shirt, arms out stretched, long hair flowing in the wind, humming the melody of Metallica's *Sandman* to the beat of the anvils?

Pythagoras believed the scientific law behind the anvil harmony could be applied to music. He found the anvils to be simple ratios of each other; one half the size of the first, another two-thirds the size, and so on. He postulated that these ratios were the root of the rhythmic harmonics he heard permeating blacksmith alley.

Similar efforts eventually led to the codification of classical music using musical notation. The goal was to improve musical integrity by capturing and authenticating the composer's intent and minimize performance improvisation and interpretation.

Nineteenth century musical notation intensified in detail and quantity, giving rise to unintended consequences. Improvisation – the mother of musical invention – gradually evolved to a relatively minor role in classical music, in sharp contrast to Japanese traditional music and jazz, where improvisation is central. Gradually, classical music developed into a stagnant genre, short on new ideas and concepts and long on repeated esoteric interpretations of century-old music from daisy-pushing composers – great music but not new music. Granted, the modern classical music era produced Debussy, Rachmaninoff, Gershwin, Copland, and Bernstein, but it pales in comparison to the heyday of the classical and romantic eras that we continually return to.

Ironically, improvisation played an important role in classical music development during the Baroque period in the form of the cadenza. No, not the legless renaissance sideboard your grandmother has in her parlor; that is a credenza. A cadenza is a passage found mostly in concertos designed to allow virtuoso artists to exhibit their skills. Traditionally, the cadenza was improvised by the composer or a virtuoso artist to make each performance unique and spawn new musical concepts in the process.

Go back to Bach's Brandenburg Concerto #3 and compare the first and third movements with the second. The second is more sedate and drab with two slow chords. It is believed that this was the cadenza where Bach expected one or more of the musicians to improvise over those chords. However, a drive for more consistency led to the cadenza being written by the composer or the virtuoso beforehand, curbing spontaneity and creativity.

So, which way will the modern day Pythagoreans take us with IA? Will their controls stagnate or liberate? Yes, information access must be certified; data cannot be changed without proper authorization; users and objects need to be genuine – not forged; information, systems, and security need to be available and functioning and, yes, we need to limit transaction repudiation. However, as we implement these safeguards, please remember balance.

Remember – your engineers grew up connected and mobile. They do more with a cell phone than you do with your laptop. They have passion and dreams they want to pursue on the fly through social and professional networks. Don't stifle that energy: harness it.

Be safe, be protective, and add structure and integrity to your systems. However, when your staff's passion goes from Edelweiss [1] to Kewpie Station [2], be sure your protective structures fan, rather than extinguish, the flames of innovation and ingenuity. Design engineering cadenzas in your process for your virtuosos to create, improvise, and dazzle your customer.

Remember, the intent of information, like music, is to connect people. The music is all around us; all you have to do is listen [3].

—Gary A. Petersen
Arrowpoint Solutions, Inc.
gpetersen@arrowpoint.us

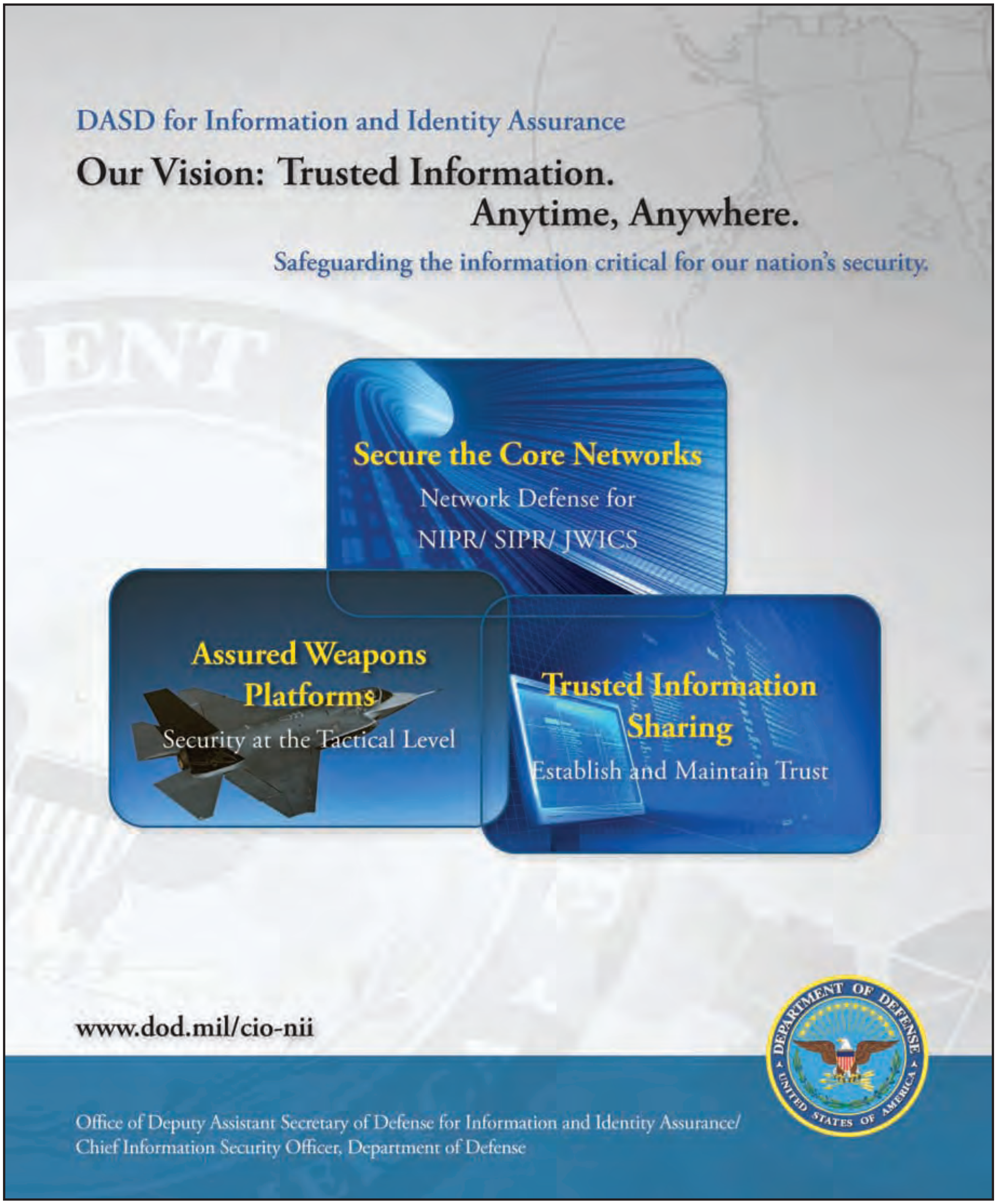
References

1. Rogers, Richard, and Oscar Hammerstein. "Edelweiss." The Sound of Music.
2. King, Kaki. "Kewpie Station." Everybody Loves You. Velour, 2003.
3. August Rush. Dir. Kirsten Sheridan. Perf. Freddie Highmore, Keri Russell, Jonathan Rhys Meyers. Warner Bros., 2007.

Can You BackTalk?

Here is your chance to make your point, even if it is a bit tongue-in-cheek, without your boss censoring your writing. In addition to accepting articles that relate to software engineering for publication in CrossTalk, we also accept articles for the BackTalk column. BackTalk articles should provide a concise, clever, humorous, and insightful perspective on the software engineering profession or industry or a portion of it. Your BackTalk article should be entertaining and clever or original in concept, design, or delivery. The length should not exceed 750 words.

For a complete author's packet detailing how to submit your BackTalk article, visit our Web site at <www.stsc.hill.af.mil>.



CrossTalk / 517 SMXS/MXDEA
6022 Fir AVE
BLDG 1238
Hill AFB, UT 84056-5820

PRSRT STD
U.S. POSTAGE PAID
Albuquerque, NM
Permit 737

CrossTalk is co-sponsored by the following organizations:

NAVAIR

Homeland Security