14/3

Volume 14 Number 3 • **Summer 2011**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals

IA in Acquisition

also inside

IATAC

contents

About IATAC and the *IAnewsletter*
The *IAnewsletter* is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a Department of Defense (DoD) sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), and Assistant Secretary of Defense for Research & Engineering ASD(R&E).

Contents of the *IAnewsletter* are not necessarily the official views of or endorsed by the US Government, DoD, DTIC, or ASD(R&E). The mention of commercial products does not imply endorsement by DoD or ASD(R&E).

Inquiries about IATAC capabilities, products, and services may be addressed to—

IATAC Director: Gene Tyler
Inquiry Services: Ryan Skousen

If you are interested in contacting an author directly, please e-mail us at *iatac@dtic.mil*.

***IAnewsletter* Staff**
Chief Editor: Gene Tyler
Assistant Editor: Kristin Evans
Art Director: Tammy Black
Copy Editor: Alexandra Holt
Editorial Board: Al Arnold, Angela Orebaugh, Dr. Ronald Ritchey
Designers: Tammy Black, Michelle Deprenger, Lacey Olivares, Donald Rowe

***IAnewsletter* Article Submissions**
To submit your articles, notices, programs, or ideas for future issues, please visit *http://iac.dtic.mil/iatac/IA_newsletter.html* and download an "Article Instructions" packet.

***IAnewsletter* Address Changes/Additions/Deletions**
To change, add, or delete your mailing or e-mail address (soft-copy receipt), please contact us at—

IATAC
Attn: Peggy O'Connor
13200 Woodland Park Road
Suite 6031
Herndon, VA 20171

Phone: 703/984-0775
Fax: 703/984-0773

E-mail: *iatac@dtic.mil*
URL: *http://iac.dtic.mil/iatac*

Deadlines for Future Issues
Winter 2011: Sept 30, 2011

Cover design: Tammy Black
Newsletter design: Donald Rowe

in every issue

IATAC Chat

Gene Tyler, IATAC Director

The entire edition this quarter focuses on a topic that I believe is of the utmost importance for information assurance (IA) professionals: ensuring products assessed into the Department of Defense (DoD) inventory are IA compliant. There are many governing documents that highlight this need, such as the DoD IA Strategy. One of the five pillars of this strategy is to "Transform and Enable IA Capabilities." One objective to this goal is "ensuring IA is integrated and sustained in all programs throughout the lifecycle." Another governing document, DoD Instruction 8580.1, states that "IA shall be implemented in all system and services acquisitions…throughout the entire life cycle of the acquisition." Over the years, I have heard comments like IA cannot be "bolted on" –very true; it must be built or "baked" in. The truth is that we must ensure IA is integrated during design, implementation, and with each product improvement (during the life cycle). We must also have a trained and qualified workforce to achieve success.

There are many resources to help those who are serious about making our products more secure. I encourage readers to learn more about what the Defense-wide Information Assurance Program (DIAP) is doing. Defense Acquisition University (DAU) is also heavily vested in imbedding IA into products. In fact, if you search for "DoDI 8580.1" on Google, a DAU link on "Information Assurance: Regulatory Requirements for IA" pops up. This information is definitely worth checking out. And there is more, just ask us at IATAC.

Within this edition of the *IAnewsletter* are a variety of perspectives on IA and acquisition. They highlight the importance of ensuring both are fully integrated and will allow our readers to understand just how negative the impacts can be if IA and acquisition are dealt with separately.

The Department of Defense Trusted Mission Systems and Networks (TMSN) Directorate team authored our feature article, "DoD Advances Supply Chain Risk Management Efforts." This article underscores the IA risks involved in managing the globalized supply chain that feeds today's information and communications technology (ICT) infrastructure. Integrating IA "in all system and services acquisitions" means ensuring every link in the ICT supply chain is strong, and TMSN is committed to advancing the policies that help accomplish this task across all sectors.

TMSN's article also highlights several Federal Supply Chain Risk Management References, one of which is IATAC's State of the Art Report (SOAR), Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain. IATAC developed this free report to help the IA and acquisition communities understand supply chain risks and how to develop risk mitigations accordingly. Please contact us at *iatac@dtic.mil* if you are interested in obtaining a free copy.

Of course this edition also includes articles about new IA developments across academia and private and public sectors. Integrating IA and acquisition requires cybersecurity solutions to continue to evolve, and we are fortunate to publish contributions by IA subject matter experts who are paving the way!

In September 2010, the Under Secretary of Defense for Acquisition, Technology and Logistics (AT&L), the Honorable Ashton B. Carter, issued a memorandum to Defense Acquisition Professionals on "Better Buying Power: Guidance for Obtaining Greater Efficiency and Productivity in Defense Spending." The title of this memorandum says it all! I believe that fully integrating IA into the acquisition life cycle is one critical step to achieving the efficiencies this policy outlines. The articles included in this edition of the *IAnewsletter* provide a small sampling of the thought leadership helping us move forward in a positive direction.

I always encourage our readers to submit articles sharing their perspectives on various IA topics. And, if you want to know more about this or other IA topics, please feel free to contact us at *iatac@dtic.mil*. I look forward to continuing this dialogue with the IA community.

DoD Advances Supply Chain Risk Management Efforts

The Supply Chain Challenge

Continued globalization marks today's information and communications technology (ICT) marketplace. This trend allows the United States Government (USG) and the Department of Defense (DoD) to take advantage of new markets, increased technological advancement, and cost efficiencies. DoD's mission-critical systems and networks extensively leverage commercial, globally interconnected, globally sourced ICT. While globally sourced ICT provides innumerable benefits to DoD, it also provides our adversaries with increased opportunity to compromise the supply chain to access or alter data and intercept or deny communications. Even though the risk of such a supply chain attack may be tolerable for many consumers of commercial ICT, the DoD cannot ignore these risks to its national security missions.

Globalization not only introduces risks related to manufacturing, it stretches across design, production, distribution, operation and maintenance, and disposal of a system or component since many companies based in the U.S. outsource numerous parts of the system life cycle overseas. All of these life cycle stages are vulnerable to exploitation by malicious actors, who may collect information; deny, disrupt, or otherwise degrade the function; and who use or operate the item or system.

DoD represents a small portion of the commercial ICT market; therefore, it is unlikely its unique high assurance requirements can drive the development of commercial off-the-shelf products. The DoD, however, is taking a proactive risk management approach to address this issue, enhancing the acquisition process in light of the changing global market to ensure processes are strong and risk aware. Instead of imposing strict regulatory provisions on ICT developed or produced in other countries, the DoD instead focuses on adapting its risk management to the market environment, employing measures and techniques that do not restrict access to the global market.

The DoD Approach

The DoD engages in efforts to assure critical systems, networks, and components and continues to introduce and refine guidance policies and procedures. In October 2003, the Deputy Secretary of Defense released a memorandum establishing a Defense Trusted Integrated Circuits Strategy (DTICS) to ensure access to leading edge and trusted commercial suppliers and critical integrated circuits for use in certain key weapons, intelligence, and defense systems. The DoD has since expanded its approach to a "defense-in-breadth" approach that addresses risk management throughout the system life cycle.

Between 2006 and 2008, the DoD, led by the Under Secretary of Defense for Acquisition Technology and Logistics (USD[AT&L]) and the Assistant Secretary of Defense for Networks and Information Integration(ASD[NII])/DoD Chief Information Officer (CIO) formulated its strategy for achieving systems assurance and participated in several studies regarding trustworthy ICT, including two Defense Science Board studies. The Comprehensive National Cybersecurity Initiative (CNCI), launched through National Security Presidential Directive 54/Homeland Security Presidential Directive 23 has driven the most recent efforts in 2008. The CNCI Initiative 11 directed the government to "develop a multi-pronged approach for global supply chain risk management." [1] Through this top level leadership-driven tasking, the government developed a strategy and implementation plan to provide the federal departments and agencies with a toolset to better manage and mitigate ICT risk across the life cycle of systems, networks, and components.

This top-down endorsement paved the way for a DoD Directive Type Memorandum (DTM): Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems. This DTM officially established a DoD SCRM policy. It

directed that supply chain risk be addressed throughout the system life cycle and required the incremental SCRM roll-out in Fiscal Year 2009 and FY 2010 with pilot programs, with full operating capability by FY 2016.

The DoD's strategy for achieving trustworthy defense information and weapons systems in light of supply chain risk contains the following core elements:

1. **Prioritize scarce resources based on mission dependence**—Allocate the DoD's systems assurance resources based on their criticality and risk of attack.
2. **Plan for comprehensive program protection**—Employ program protection planning to identify and protect critical components, technologies, and information using the full range of cost-effective best practices, including SCRM key practices.
3. **Detect and respond to vulnerabilities in programmable logic elements**—Invest in enhanced vulnerability detection research and development and transition such analytical capabilities to support acquisition.
4. **Partner with industry**—Collaborate with industry to develop commercially reasonable standards for global sourcing and SCRM and identify leading edge commercial practices and tools.

Implementation of the DoD Approach

In support of CNCI Initiative 11 and in accordance with DTM-09-016, the ASD(NII)/DoD CIO and USD(AT&L) lead the incremental implementation of the DoD SCRM program. This effort began in earnest with pilots within DoD in FY 2009 and FY 2010 through its Trusted Mission Systems and Networks (TMSN) directorate, formerly the Globalization Task Force. In line with the DoD's strategy, the SCRM pilot program objectives were to evaluate SCRM and secure systems engineering best practices; utilize threat-informed technical mitigations; and develop enhanced acquisition planning and practices.

Initial piloting activities focused on standing up organizational structures and cultivating the best practices for supply chain risk management. For example, the SCRM Program Management Office was established within ASD(NII)/DoD CIO to provide oversight and coordination as well as direct involvement for the SCRM pilots. Second, the Army, Navy, and Air Force established Centers of Excellence (COEs) with the authority to represent its component service with regard to SCRM communications and piloting.

In addition to standing up the organizational components and processes for SCRM, the program conducted more than 30 pilots in FY 2009 and FY 2010. These pilots focused on

Implementing SCRM: 2003-2010

2003—Deputy Secretary of Defense released the memorandum establishing a DTICS.

2004—The Trusted Foundry Program for Integrated Circuits was established.

2006—DoD established the Software Assurance Tiger Team.

2006—The Committee on National Security Systems (CNSS) Global IT Working Group released a report proposing the "defense-in-breadth" approach.

2008—The National Defense Industrial Association released the Engineering for System Assurance guidebook.

2008—The President launches CNCI, which called for the supply chain risk management approach across system life cycles.

2009—DoD established the Department-wide SCRM policy through DTM 08-048, SCRM to improve the Integrity of Components Used in DoD Systems, directing DoD components to implement SCRM within all critical information systems and weapons systems by FY 2016.

2010—The DTM for SCRM was updated through DTM-09-016. The Information Assurance Technology Analysis Center (IATAC) State of the Art Report (SOAR) on Security Risk Management of the Supply Chain was published.

acquisition of systems and commodities, vulnerability assessments of major acquisition programs, program protection plan reviews, Pathfinder assessments, and SCRM-enhanced test and evaluation processes. These pilot programs helped establish the foundational structure from which a fully operational SCRM capability is built.

For example, during vulnerability assessments, the DoD analyzed systems engineering practices, system designs, threats related to suppliers and supply end items, and program protection activities. Pathfinder pilots—which have continued after the pilot period to support full scale implementations—focus on assessing supply chain risk through a process called criticality analysis. Criticality analysis involves identifying and prioritizing mission threads, identifying critical system functions, and then mapping those functions to critical logic-bearing components for warfighting systems. This information is then used to make acquisition and design risk management decisions. The ASD(NII)/DoD CIO, USD(AT&L), Army, Air Force, and Navy are all working together to further refine the criticality analysis process.

Pilot programs implemented supply chain risk-enhanced systems engineering and acquisition practices detailed in the SCRM Key Practices and Implementation Guide. This guide provides a set of business and technical practices, which organizations that acquire goods and services can implement to proactively protect the supply chain against exploitation, subversion, or sabotage.

A major focus of the piloting process was for programs to validate and determine the effectiveness of the key practices defined in the guide. These key practices are in the process of being updated and streamlined based on pilot program findings (detailed in Figure 1).

The pilot project results are currently being analyzed for any needs, gaps, or impediments in policies, processes, or technologies necessary to implement SCRM robustly throughout the DoD. This analysis provides an empirical foundation on which resource requests and policy changes can be determined. DoD is preparing a report that captures lessons learned from the pilot projects and outlines the recommended way forward for full scale implementation. Overall, the pilot programs validated the DoD's existing strategy for assuring trust in its mission critical systems and networks.

Though the initial pilot phase ended in FY 2010, DoD is continuing to build upon the incremental roll-out of those activities through the continued stand-up and refinement of the COEs, continued Pathfinder pilots with the military services, and the expansion of agency pilots. As these capabilities grow, DoD will continue to implement SCRM concepts in policy and procedures; provide resources to SCRM COEs to provide systems engineering and acquisition support; enable threat-informed SCRM tests and evaluations; and implement SCRM training.

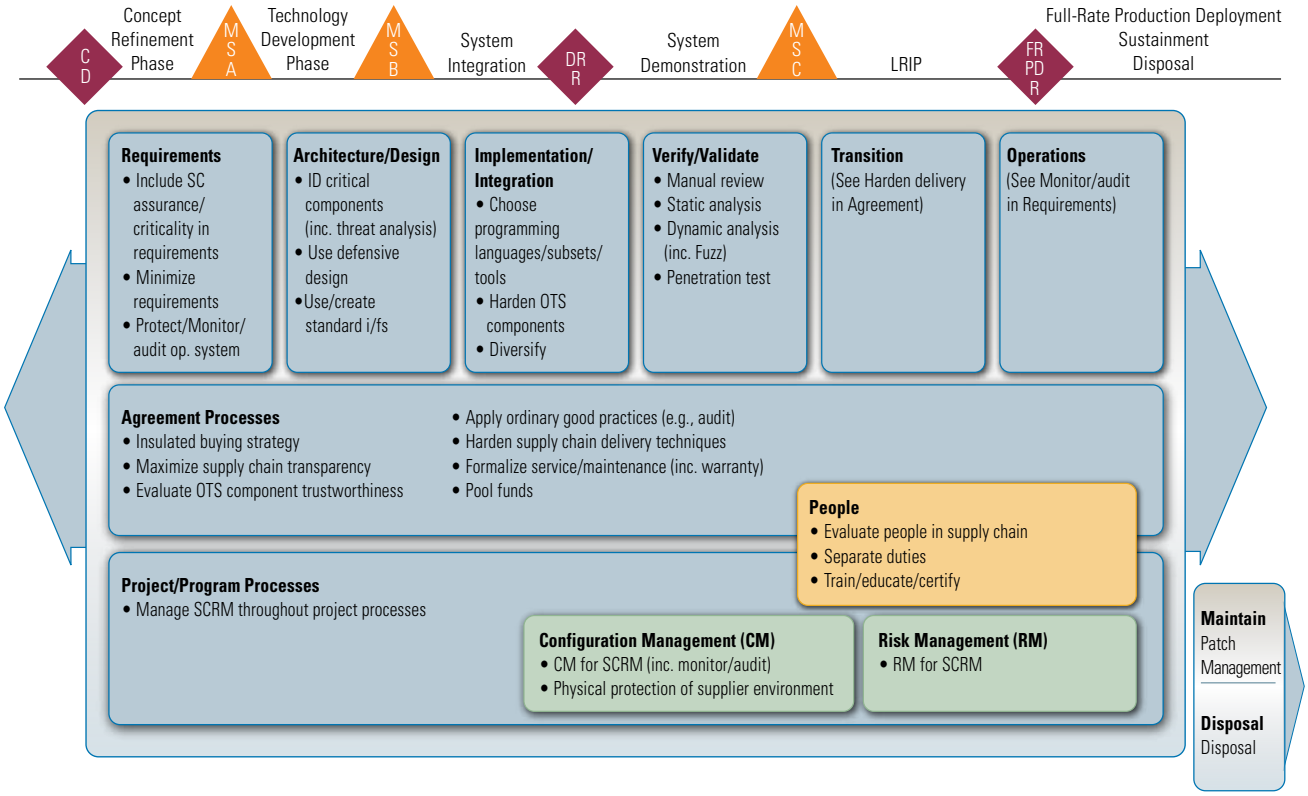


Figure 1 SCRM Key Practices in the DoD System Acquisition Life Cycle

Collaboration with Industry

DoD engages in a robust collaboration with industry to collect, analyze, and share SCRM best practices and to better understand the level of risk the government accepts when procuring ICT from commercial suppliers and integrators. The DoD strategy is to actively engage industry by participating in key standards development organizations (SDOs) and reaching out at major community events; soliciting and collecting interagency and industry feedback; and working to develop and incorporate industry best practices into work products at the national and international levels. In addition, DoD, Department of Commerce/National Institute for Standards and Technology (NIST), and Department of Homeland Security's National Cyber Security Division sponsor the DHS-led Software Assurance (SwA) Program. The sponsors host quarterly forums and working groups to bring together members of government, industry, and academia with a vested interest in SwA to discuss and promote integrity, security, and reliability in software development and use.

One of the key standardization and outreach goals is to facilitate development and adoption of commercial global sourcing standards to baseline industry practices for DoD and other government acquirers of ICT products and services as well as to establish industry-acceptable best practices for monitoring compliance with these requirements. To achieve this goal, TMSN is engaged in several key national and international standardization efforts.

To focus its international standardization efforts, DoD has identified relevant ongoing efforts within the International Organization for Standardization (ISO) and other key SDOs and is moving forward to influence the content of several key standards as well as developing an umbrella-type standard to cover ICT SCRM-specific requirements and practices. The DoD chairs the ICT SCRM Ad Hoc Working Group, which includes more than 40 government and industry organizations under the auspices of Cyber Security 1, chartered with representing U.S. interests to ISO/International Electrotechnical Commission (IEC) Joint Technical Committee 1 Subcommittee 27 (SC 27) on information technology (IT) security techniques. Based on the working group recommendations, in November 2009, the U.S. proposed to SC 27 to develop an ICT SCRM standard. After a yearlong study period on the subject, SC 27 approved a new standard in October 2010: ISO/IEC 27036 - Information Technology – Security Techniques – Information Security for Supplier Relationships. The standard is being developed in collaboration with the Information Security Forum, a global non-profit organization with 300 corporation members that identifies the global supplier relationship challenge as one of its top priorities. To ensure that the new standard appropriately references related content from other ISO committees without duplication, SC 27 established a number of liaison relationships with relevant committees addressing a broad variety of subjects including system and software engineering, fraud countermeasures and controls, and anti-counterfeiting tools. In addition to helping establish a new standard, the working group has worked to integrate ICT SCRM content into a number of other key standards.

One of the key standardization and outreach goals is to facilitate the development and adoption of commercial global sourcing standards to baseline industry practices for DoD and other government acquirers of ICT products and services.

With NIST, the DoD co-leads the CNCI SCRM Life Cycle Processes and Standards Working Group 2 (WG2), which collects information about governmental SCRM activities, lessons learned, and best practices that might contribute to SCRM standardization and institutionalization of SCRM capabilities. WG2 also provides coordination on the draft NISTIR 7622 – Piloting Supply Chain Risk Management for Federal Information Systems, which will provide a set of practices for federal agencies that can be referenced or used for high-impact federal information systems (FIPS-199, Federal Information Processing Standards). NISTIR 7622 practices—based on those identified in the DoD SCRM Key Practices and Implementation Guide—are intended to promote the acquisition, development, and operation of information systems or system-of-systems to meet cost, schedule, and performance requirements in today's environment with globalized suppliers and active adversaries. Integrated within the information systems development life cycle, these practices provide risk-mitigating strategies for the acquiring federal agency to implement.

DoD is also engaged in The Open Group's Trusted Technology Forum (TTF). The TTF strives to provide a collaborative, open environment for technology companies, customers, government, and supplier organizations to create and promote guidelines for manufacturing, sourcing, and integrating trusted, secure technologies. These guidelines will ultimately shape global procurement strategies and best practices to help reduce threats and vulnerabilities in the global supply chain. TTF is scheduled to publish

several products during the next year including the Trusted Technology Provider Framework and harmonize it with other standards.

DoD collaborates with a variety of other government, industry, and public/private activities to solve the ICT SCRM challenge, including the IT Sector Coordinating Council; the Partnership for Critical Infrastructure Security SCRM Working Group; and New York University's International Center for Enterprise Preparedness Supply Chain Integrity Working Group.

Through the next 3 years, the DoD plans to strive to move these efforts forward with the goal of making a family of related ICT SCRM standards available for government and industry to use to establish mature relationships with ICT service and product providers. The ultimate goal of the standardization efforts is to help raise the bar of best practices globally and to help create a more transparent environment for acquirers of ICT services and products.

What's Next

In addition to advocating for international SCRM standards, DoD continues to march towards full scale implementation of DoD's SCRM program while participating in CNCI and partnering with CNSS and other agencies to advance SCRM efforts across all mission critical government systems and networks. Within the DoD, a key objective for 2011 is developing an integrated set of information assurance and acquisition policies to reflect SCRM concepts. ASD(NII)/DoD CIO and USD(AT&L) plan to continue to support the military services and defense agencies as they build out their capabilities and provide guidance and support to programs on how to identify and manage risk they may have already accepted. Training, education, and awareness efforts are important components of this effort.

The DoD's strategy for moving forward reinforces its commitment towards achieving a cohesive, enterprise-wide SCRM risk management solution.

Implementing SCRM in Your Organization

There are a variety of resources for federal agencies working to integrate supply chain risk management into their organization's overall risk management practices. Private sector ICT product and service providers, including federal contractors, can also benefit from reviewing and implementing some of these practices since the private sector is an important partner in building and maintaining trusted systems and networks. ■

Federal Supply Chain Risk Management References

The following documents provide systems security engineering guidance, SCRM policy, and detailed risk management best practice for use in commercial or government systems:

- *Draft* NISTIR 7622, *Piloting Supply Chain Risk Management for Federal Information Systems*, June 2010.
- National Defense Industrial Association (NDIA) System Assurance Committee. 2008. *Engineering for System Assurance.* Arlington, VA: NDIA.
- Directive Type Memorandum 09-016, *Supply Chain Risk Management to Improve the Integrity of Components Used in DoD Systems,* March 25, 2010.
- SCRM Program Management Office, Trusted Mission Systems and Networks, OASD(NII)-CIO/ODASD(CIIA). *Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program,* February 25, 2010.

In addition, IATAC released a SOAR on supply chain risk management titled *Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain.* This SOAR examines both threats to supply chain processes and from supply chains that have been compromised and serves as a reference on supply chain security for government, industry, and academia.

Federal IT Security References

The following documents provide a foundation of federal IT security practices or provide detailed guidance specific to managing risks inherent in the IT product or services supply chain.

- CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems,* October 2009
- NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009 (includes updates as of May 1, 2010).
- NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* February 2010.

The Trusted Missions Systems and Networks (TMSN) team oversees the implementation of the strategy for mitigating national security risks to DoD weapons systems and information systems arising from the globalization of ICT. In addition to leading DoD efforts in SCRM, TMSN leads DoD's analysis of direct foreign investment transactions involving ICT and U.S. telecommunications infrastructure. TMSN also works with interagency and industry to understand and manage conditions related to SCRM in critical telecommunications infrastructure and trade and economic policy underpinnings to U.S. ICT competitiveness.

About the Authors

The following TMSN Directorate team members contributed to this article: Mitch Komaroff (Director), Jenine Patterson, Don Davidson, Annette Mirsky, and Joe Wassel. A special thanks to Nadya Bartol, Serena Chan, Sarah Corwin, James Grimes, Geoff Grogan, and Don Whitten who also contributed.

References

1. *http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative*

Bridging DoD IA Requirements and Commercial IA Solutions

Currently, the Department of Defense (DoD) faces an array of increasingly lethal cyber threats from nation states and non-governmental actors that requires evolution of the information assurance (IA) posture of information technology (IT). This landscape requires DoD IA government officials and operators to stay abreast of the latest technological developments to protect and defend mission critical IT. There are several Commercial Innovation and Integration (CII) programs for sourcing, certifying, and making new technology available. The DoD IA Connect program, an ongoing initiative from the DoD Chief Information Office (CIO), focuses on improving the matchmaking process between DoD IA requirements and the number of IA vendor solutions commercially available today. DoD CIO's IA Connect program creates awareness and promotes knowledge sharing within the DoD IA community of emerging IA technologies and provides opportunities for vendors to demonstrate their innovative capabilities.

IA Connect provides a single DoD interface with IA vendors to share information about their technologies within DoD. By creating a focal point for vendor communication and coordination, DoD has created a knowledge base from which to create and share dialog about the application of IA products within DoD, reducing point-in-time efforts and driving collaborative activities to better understand the deltas between DoD needs and the maturity and availability of IA products. Information gathered through IA Connect is posted on the online IA Connect Knowledge Center where users can access this knowledge and exchange insights on the capabilities and use of products and services.

IA Connect tracks more than 85 product and service profiles and adds to the base every week. For these existing product profiles, users are encouraged to add relevant data to further augment the DoD body of knowledge. If users cannot find information about related products or services, they can be referred to IA Connect for initial handling, background research, due diligence, and tracking. After an initial profile has been generated, it is circulated within the community for interest. If there is interest in a potential vendor, the IA Connect program facilitates meetings or demonstrates their product or service to interested parties. Direct vendor referrals and inquiries to the IA Connect coordinator at *IAConnect@osd.mil*.

For additional information about the IA Connect program, visit *https://nii.iaportal.navy.mil/login.htm*. Access requires a Common Access Card and a military e-mail address. The IA Connect program also publishes a biweekly newsletter with site updates including new vendors, products, and services posted to the Knowledge Center and a list of upcoming events.

The IA Connect program recently established a Vendor Days series as a regular forum for featuring vendor technologies and services to the DoD community. If you are interested in attending IA Connect Vendor Days, e-mail the IA Connect Team at *IAConnect@osd.mil*. ■

Figure 1 IA Connect Knowledge Center

Information Assurance and Acquisition

by Tim Denman, Deborah Williams, and Vijaykumar Rachamadugu

"There's a war out there old friend, a world war. And, it's not about who's got the most bullets; it's about who controls the information: what we see and hear, how we work, what we think. It's all about the information." [1]

Information Warfare is being acted out on battlefields and in war rooms across the world. Its implications for the Department of Defense (DoD) acquisition are enormous. If our troops are to be effective in combat, they must have information superiority and absolute trust in the integrity of the systems and networks that move and manage that information. Information assurance (IA) plays a crucial role in this mission as it enables and protects information as well as the systems and networks in which it resides.

Both IA practitioners and information technology (IT) users often misunderstand the role of IA as a protector and enabler of information. IA professionals often feel they are put in "no win" situations as they are asked to protect the DoD network. In turn, IT users often view IA professionals as disablers of their ever-so-critical information. Recent restrictions on USB drives due to security issues, scores of banned websites, and ever-tightening access controls have only served to exacerbate these issues. For IA to better protect and enable the DoD network, the IA professional and DoD leadership should work to keep IA at the forefront throughout the acquisition life cycle. It is necessary for the culture of IA within the DoD to change and for acquisition leadership, IA professionals, and IT users in general to work together across the DoD to facilitate change. Recommendations and information found in the Information Assurance Policy Crosswalk Working Group Report, the Software Assurance Forum for Excellence in Code, and Information Assurance Technology Analysis Center (among others) provide critical components to unify acquisition's response to IA threats across the DoD.

Changing the IA Culture within DoD Acquisition

The following recommendations to change the IA culture within DoD acquisition are detailed in the remainder of this article:

1. Greater involvement of IA professionals throughout the acquisition life cycle;
2. Enhanced leadership commitment and understanding of IA and the IA process;
3. Further integration of IA into the systems engineering and contracting process;
4. Moving beyond IA awareness for IT users to prevention and detection; and
5. Increased focus on software assurance.

Greater Involvement of IA Professionals throughout the Acquisition Life Cycle

As noted above, there is often an adversarial relationship between the IT user, DoD leadership, and the IA professional. Much of this conflict is because the IA professional has the reputation as someone who gets involved only after the deployment of an IT system and restricts access to information. For this view to change, IA professionals should have greater involvement throughout the acquisition life cycle.

The focus of the IA professional shifts as the acquisition life cycle progresses and the life cycle system moves into the deployment phase. After deployment, the IA professional focuses more on day-to-day secure operations within the fielded environment. As such, the emphasis shifts away from engineering and toward the management of network and host defense mechanisms, managing connection processes, ensuring that an array of IA policies are in place and being followed, and adhering to the never-ending patch management process. Certification and accreditation processes and issues are also a focal point for IA professionals across the deployment and operational phases.

When IA professionals participate in the early stages of the acquisition process through system security engineering activities, their

If our troops are to be effective in combat, they must have information superiority and absolute trust in the integrity of the systems and networks that move and manage that information. Information assurance plays a crucial role in this mission as it enables and protects information as well as the systems and networks in which it resides.

contributions build appropriate security measures into the design and operation of the acquisition system. These efforts allow them not only to advise and educate DoD leadership and potential users but also to gain a better understanding of the acquisition process and craft solutions to IA threats with a greater understanding of the system's usage and operational environment. The involvement of IA professionals in integrated product teams and integrated test teams as well as providing subject matter expertise before contract award (pre-milestone B) is crucial for the long-term success of acquisition programs.

The numbers, role, and scope of responsibilities for DoD IA professionals have evolved significantly over the last 15 years. In 1999, individuals with the Certified Information Systems Security Professional (CISSP) certification numbered in the low hundreds; as of July 20, 2010, 67,744 members hold the CISSP certification in 134 countries. [2] The number of people in the information and systems security field has also increased as well as the range of their roles and responsibilities. The IA discipline has matured into complementary specializations that fit within the planning, development, deployment, and management/maintenance phases of DoD acquisition efforts.

The skills and focus areas of the IA professional are differentiated across the acquisition life cycle, and those focus areas should be optimized for both the system's life cycle phase and operational environment. Significant improvements in a system's security posture and often-lower life cycle costs can be realized when system security engineers engage in the design and development phases.

Enhanced Leadership Commitment and Understanding of IA and the IA Process

Partly because of negative publicity generated by IA breaches, leadership's understanding of the importance of IA has increased significantly in recent years. In most cases, IA funding is no longer the first cut made in an acquisition program and IA awareness programs are now mandatory. Unfortunately, IA awareness progress is not keeping pace with the ever-increasing threat. If IA is to take sufficient strides, the culture of leadership must significantly change. Acquisition leaders should embrace IA and look for ways to involve IA throughout the acquisition process. IA training for acquisition leaders beyond the typical awareness programs is critical. The IA community should consider developing 2 to 3 day training courses that provide a walkthrough of programmatic IA scenarios as well as IA case studies as ways to facilitate this change. The need for greater accountability when program managers or other leaders violate IA rules is another key step in this process.

In addition to leadership understanding IA, the systems engineering and acquisition staff have to recognize the importance of IA. The IA Policy Crosswalk Working Group (IPCWG) Report found that "Government workforce needs more qualified people with requisite skills to support IA in systems acquisition and Test and Evaluation." [3] Subsequent recommendations call for a review of DoD IA curricula to identify IA training gaps that exist in preparing systems engineering and program management professionals to participate in all phases of the systems acquisition process. In specific terms, the IPCWG Report recommends that IA curricula address IA skills needed for successful IA Systems Engineering in the early phases of systems engineering.

Further Integration of IA into the Systems Engineering and Contracting Process

To address comprehensive security of systems being acquired, IA should be added as a systems engineering technical management process in the DoD framework. The IPCWG Report recommends, "IA capabilities and requirements should be addressed in the early Systems Engineering Technical Reviews and translated into robust system requirements, RFPs, and the IT system preliminary design." [4] IA must evaluate each system acquisition effort to determine the particular information and processes to be protected and to determine appropriate measures for managing that protection. The systems engineering process should incorporate these measures.

Fortunately, IA experts across industry, government, and academia, agree on the need for more formal integration of IA into the systems engineering process. Two specific areas that were cited by the IPCWG Report and elaborated on in recent conferences on the topic include the IA Concept of Operations (CONOPS) development and integration and IA requirements

The most important ingredient in providing for greater IA protection is a change in culture. This cultural change should precede real IA change and subsequent improvement.

definition, allocation, integration, and testing. [5]

The development of an IA CONOPS should precede the development of systems and subsystems requirements and occur well before the Preliminary Design Review (PDR). The IA CONOPS development will facilitate scenario-based planning to mitigate attacks, disruptions, faults, and failures across the system's IT infrastructure. A critical portion of the IA CONOPS would incorporate a Mission Dependency Analysis (MDA) that identifies critical component functionalities and determines both asset and mission dependencies (*i.e.,* those components or subsystem components within a system that serve as potential single points of failure or whose functionality is critical for the successful execution of the system's mission). Once the MDA identifies these dependencies, it can also identify and integrate appropriate safeguards into the system's design. In addition, the foundation of a well-documented set of mission dependencies and their planned safeguards offers an excellent testing venue that IA can leverage later in the system's life cycle.

Common practices in today's acquisition communities do not recognize and integrate system security engineering functions early in the design and development process. IA makes significant contributions in these early life cycle phases when IA defines the requirements, allocates them to the system architecture, and integrates them into the systems engineering baseline of functional requirements, yielding multiple benefits. By integrating appropriate security measures into the design and development process, security postures are optimized and cost impacts are minimized. The verification of these explicitly defined criteria also can be integrated into the existing systems engineering processes, providing both life cycle cost efficiencies and formal documentation.

To ensure that the systems engineering process incorporates IA, the IA requirements must be included in the contracting process. The IPCWG Report recommends that "the Request for Proposal Statement of Work should direct contractors to address IA during PDRs, Critical Design Reviews, and all technical reviews." [6]

Moving beyond IA Awareness for IT Users to Prevention and Detection

The DoD currently requires all employees to take an online IA awareness course on a yearly basis. While this training provides useful information, it is only an initial step. The typical IT user is an important line of defense in a layered defense in-depth approach especially when it relates to the insider threat. The IT user often sees the first evidence of a threat and can take steps to detect, report, and defend against information compromise. Providing incentives for reporting possible IA incidents and simply encouraging behavioral awareness is a good step in this important first line of defense.

In a great number of cases, the user will not be able to recognize the complex attack vectors that exist today; however, safe computing practices, situational awareness, and general information security and communications security

practices can go a long way to help thwart potential attacks.

Increased Focus on Software Assurance

Software Assurance (SwA) is "the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner." [7] The DoD Software Assurance Initiative was launched in 2005 and includes excellent recommendations such as partnering with industry to develop better SwA tools and employing repeatable systems engineering and test processes to mitigate software vulnerabilities. Following through with these recommendations along with consistently including SwA requirements in the contracting process (as noted in the IPCWG report) are important steps.

Just as IA CONOPS and IA requirements may be introduced into the design and development life cycle phases, SwA assessments may also be integrated into the system verification processes. The IA CONOPS, which can presume that possible software vulnerabilities exist and then help users plan for and test their mitigation, may explicitly address SwA concerns. Collectively, these practices would serve to both reduce the number of software vulnerabilities that flow into a developed system and mitigate the threats caused by vulnerabilities that may exist.

Conclusion

Perhaps surprisingly, there is no mention of the DoD Information Assurance Certification and Accreditation Process or the Federal Information Security Management Act in the recommendations above. While both of these policies are a necessary component of IA in acquisition, they do not ensure that an acquisition program has the needed amount of IA protection. The most important ingredient in providing for greater IA protection is a change in culture. This cultural change should precede real IA change and subsequent improvement. The recommendations discussed provide the beginnings of this change and, most importantly, will help enable and protect the important information systems and the exchange of information on those systems throughout the DoD. ■

About the Authors

Tim Denman | is currently the Systems Engineering and Technology Department Chairman for Defense Acquisition University in Huntsville, Alabama. He teaches classes in the IT, Systems Engineering (SE), and Production, Quality and Manufacturing career fields (as specified by the Defense Acquisition Workforce Improvement Act). Mr. Denman formerly worked as a Systems Security Engineer for the Ground-Based Midcourse Defense (GMD) program and on the GMD Certification and Accreditation team as a systems engineer. Mr. Denman earned a Bachelor of Science degree from the University of Alabama and received a Master of Business Administration (MBA) from Indiana University. He earned his CISSP certificate in 2006. He can be contacted at *tim.denman@dau.mil*.

Deborah Williams | has worked across the cybersecurity life cycle in support of Federal and DoD clients since 1999. She has performed system SE, IA management, and certification & accreditation activities for the Missile Defense Agency and supported the Army and Navy with strategic cybersecurity planning. Her areas of expertise include development and implementation of cybersecurity risk assessment methodologies. Current research interests include malware heredity identification technologies, cybersecurity management, and policy development. She holds a Master of Public Administration from the University of Alabama at Birmingham as well as a CISSP. She can be contacted at *deborah.williams@sentar.com*.

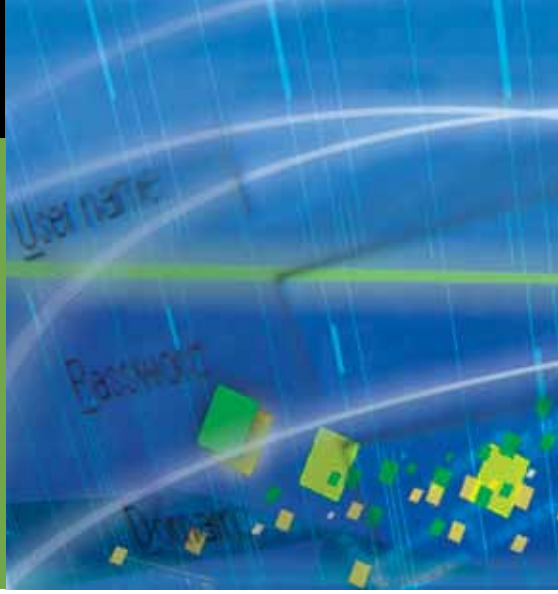
Vijaykumar Rachamadugu | has over 25 years of experience in Mission Assurance, information security, enterprise architecture, networking, and communications engineering. He holds an MBA in Finance from Virginia Tech, Master of Science (MS) in Computer Science from the Indian Institute of Technology, and CISSP certification. In 2006, he was finalist for the prestigious Information Security Executive of the year - Mid Atlantic Award. He has presented Information Security and Privacy topics at various conferences. He can be contacted at *vijayr@mitre.org*.

References

1. Sneakers. DVD. Directed by Phil Alden Robinson. 1992; Los Angeles, CA: Universal Pictures, 1992.
2. The International Information Systems Security Certification Consortium, Inc. (ISC)²®, the issuing entity of the certification.
3. IA Policy Crosswalk Working Group Report. *http://www.acq.osd.mil/dte/docs/IA_Cross_Walk_WG_Report-3-30-10.pdf*
4. Ibid
5. In October 2010, the Mitre Corporation held the "Secure and Resilient Cyber Architectures Conference" at its McLean, Virginia facility. Many presentations and papers delivered at the conference converged around these key points.
6. Ibid
7. Committee on National Security Systems. National Information Assurance Glossary. *<http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>*

A Commercial Engagement Strategy for Authorization and Access Management in Defense and Intelligence Communities

by Art Friedman and Adam Schnitzer



Over the past 10 years, the federal government has invested unprecedented resources to enhance cybersecurity capabilities. Advances in the development and adoption of network security, centralized threat identification and response, security automation, and identity assurance technologies and processes are matched only by our adversaries' tenacity in finding our weaknesses and the ever-present insider threat. According to the 2010 Cybersecurity Watch Survey of more than 500 commercial and government organizations, nearly 3,000 attacks per year are detected by the average organization. One-quarter of all cybersecurity events are committed by an insider, and more than half of the survey's respondents were attacked by insiders in 2009. More than two-thirds of the respondents admitted that, historically, insider attacks are always more costly to their organizations than external threats. [1]

As the Department of Defense (DoD) and Intelligence Communities (IC) endeavor to implement enhanced enterprise authorization capabilities, Chief Information Officers (CIOs) and Programs of Record (POR) face the challenges of implementing enterprise authorization capabilities with little guidance, limited governance, few enterprise requirements, and still-maturing technologies under severe fiscal constraints. Because of current budget limitations and the lack of consolidated and authoritative buying power, the DoD and IC are forced to implement commercial solutions in an *ad hoc* fashion, without achieving the economies of scale required for the enterprise, and without a standard set of interfaces that allow interoperability among products. It is increasingly apparent that the DoD and IC require a comprehensive strategy to influence the development of commercial products. This strategy must address the gap between technology concept, maturation, and adoption; demand interoperability while incentivizing competition; allow for the evolution of capabilities; and make sure solutions are secure, resilient, cost effective, and easy to use.

The Commercial Engagement Strategy

The tenets of a commercial engagement strategy are presented below outlining the five objectives required by the DoD and IC for successful commercial engagement and influence over technology development. By following these recommendations, it is anticipated that development and adoption of enterprise authorization capabilities can progress more rapidly and provide enhanced abilities to protect mission-critical information and services from external and internal threats.

Objective 1—Establish Clearly Organized Authorities and Governance for DoD/IC Authorization Capability Development and Implementation

To achieve unity of effort for influencing commercial product vendors, clearly defined authorities within the DoD and IC are required. Coordinated directives and subordinate instructions are needed to outline roles, responsibilities, and governance structures for the development and acquisition of new technologies, adherence to standards and specifications, and establishment of testing and compliance requirements.

Current governance and authority structures are not optimal and focus on IT resources for mission systems rather than on the infrastructure and enterprise services necessary to enable advanced secure information sharing capabilities. Although the Federal CIO Council's Federal Identity, Credential, and Access Management (FICAM) effort has made initial progress in the areas of concept, architecture, and governance, detailed technology development and implementation guidance for DoD and IC entities is still needed. The IC is making significant progress through the IC Identity and Access Management (IdAM) program under the authority of the Director of National Intelligence (DNI).

Similarly, within the DoD, efforts directed by the Enterprise-wide Solutions Steering Group (ESSG) and

> The community will continue to meander in the general right direction, but if any real progress is expected, governance will need to be established and embraced. [2]

Identity Protection Management Senior Coordinating Group (IPMSCG) are enjoying concrete, if limited, successes. The ESSG is charged with providing centralized governance geared toward the assessment, validation, and implementation of enterprise-wide solutions throughout the DoD. This steering group, originally chaired by the U.S. Strategic Command (USSTRATCOM) and Joint Task Force-Global Network Operations (JTF-GNO) – now U.S. Cyber Command (US CYBERCOM) – coordinates the DoD enterprise solution efforts. The ESSG is sanctioned to provide leadership, oversight, planning, and advocacy to streamline the decision-making process of DoD combatant commands, services, and agencies. Yet the scope of the ESSG is often far greater and more diverse than its resources and authorities can adequately address, limiting its focus to just-in-time solutions that meet urgent needs. Likewise, the IPMSCG has focused primarily on identity management and protection and has recently, with the publication of the DoD Privilege Management Roadmap in January 2010, expanded its scope to provide guidance for the DoD implementation of authorization solutions.

As access control technology, standards, and enterprise capabilities become more mature, an authority or set of authorities is needed to establish guidelines to ensure interoperability for information sharing, maximizing economies of scale, and promoting a competitive and collaborative environment within the vendor community. The Unified Cross Domain Management Office (UCDMO) serves as one model, demonstrating consolidation of effort and policy alignment within a centralized governance structure. The UCDMO provides centralized coordination and oversight to all cross-domain initiatives across the DoD and IC. The policies and procedures set forth by the UCDMO authority apply to any DoD/IC program where cross domain solutions are addressed and implemented.

At the very least, an organization must come forward to serve as a clearinghouse for best practices, lessons learned, and recommended technology solutions. While a more direct study of the ideal solution is required, one thing remains certain: if we cannot answer the question of who is in charge of enterprise authorization services, then the success of implementing truly robust, fine-grained, and interoperable access control solutions throughout the DoD and IC is at risk.

Objective 2—Establish, Refine, and Mandate Standards, Specifications, and Measures of Compliance for DoD/IC Authorization Capability Interoperability

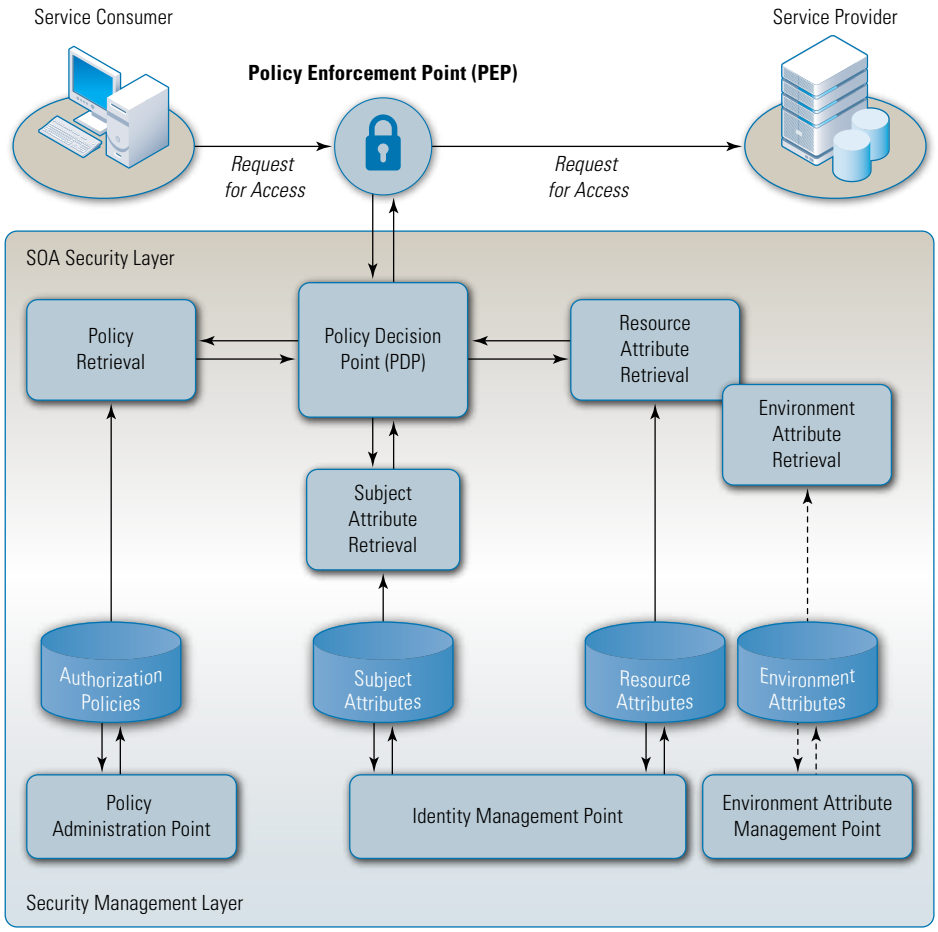
Currently, industry standards bodies are developing new access control capabilities. They have standardized policy objects that can be used to make access control decisions, create and exchange policies, and define rules to extend policy based security. This work has been performed in the Distributed Management Task Force (DMTF), the Organization for the Advancement of Structured Information Standards (OASIS), The Open Group (TOG), and other standards development organizations. Various aspects of policy schema, protocols, and languages are being standardized, which can improve the chances of interoperability in policy-based management systems. Maturing standards such as Security Assertion

Markup Language (SAML), Extensible Access Control Markup Language (XACML), and Web Services Policy (WS-Policy) provide a viable framework for vendor product development.

In 2008, the DoD and IC developed and adopted the Service-Oriented Architecture (SOA) Security Reference Architecture and Policy Decision Point, Policy Enforcement Point, and Policy Service Specifications to address one form of access control implementation – Attribute Based Access Control (ABAC) in a SOA environment (see Figure 1). These specifications seek to open the interfaces between access control components and drive toward interoperability. Although these specifications invoke the use of commonly employed and widely adopted protocols and specifications like SAML and XACML, the largest vendors have not widely adopted these or other interface-opening specifications because of the business incentives inherent in maintaining proprietary interfaces within their holistic access control solutions.

The DoD and IC are well positioned to leverage existing authorization standards and to steer future refinements to better meet their needs. An excellent model on which to pattern authorization services standards, specifications, and compliance maturation and implementation would be the National Institute of Standards and Technology's (NIST) Security Content Automation Protocol (SCAP) program. SCAP is a suite of specifications developed by the configuration management and security automation community focused on establishing a baseline of enterprise assets, verifying configuration compliance, determining vulnerabilities, and remediating devices to maintain compliance and minimize vulnerability. Vendors see the value of participation, adopt the protocol, and develop and sell their products as "SCAP-compliant."

Through vendor participation, the establishment of a portfolio of authorization specifications can make great progress toward the desired level of interoperability and capability in DoD/IC authorization services. It is important to note, however, that standards do not address all of the authorization service needs of the DoD and IC nor can they be expected to be adopted in a consistent fashion that ensures interoperability without having the proper compliance and business incentives for the vendors.



Source: DoD/IC SOA Security Reference Architecture

Figure 1 Generic ABAC authorization pattern

Objective 3—Outline and Communicate Vendor Incentives for Developing and Offering Interoperable and Compliant Authorization Solutions

A business case must be constructed to consider the economic factors associated with vendor business models. The IT research company Gartner estimates that worldwide IT spending in 2010 was $2.4 trillion. According to the federal IT research firm, Government Insights, the entire federal government accounts for just 3% of that figure – while the DoD makes up a scant 1.5% of the global IT market (see Figure 2). [3] [4] Not only are the DoD and IC resources a drop in the ocean of spending, the preponderance of current worldwide IT spending is not focused on protecting information, but rather on sharing information – growing the users' access to data for business intelligence, detecting social patterns, and increasing data mobility.

A successful engagement strategy must recognize that the vendor community is often motivated by different market forces and priorities than the federal government. The DoD and IC must recognize and embrace

these differences by observing and adopting mainstream technology trends while working with the vendor community to better communicate and maintain the "line in the sand" of DoD/IC-specific requirements. By leveraging similarly motivated market forces like the global banking, transportation, energy, or healthcare industries where protection of financial, personal, and sensitive information drives a set of requirements very similar to those of the DoD and IC, the DoD and IC can help the vendor community understand the incentives of evolving technology for a small community with specialized requirements to penetrate larger market segments and lead the way for global market technology trends.

Similarly, vendors must recognize that the "one-size-fits-all" enterprise solution does not satisfy the needs of the DoD and IC. Different mission, political, organizational authority, resource, and acquisition considerations force each component of the DoD and IC to treat its portion of the DoD/IC enterprise as a self-sufficient enclave. While this makes security and asset management simpler, it sharply contrasts the notion of information sharing espoused by the 9/11 Commission Report. Individual organizations purchase access control solutions that meet their security needs, are within their budget, and interoperate with their systems. While this model has been fairly lucrative for the vendors involved, the proprietary nature of the component interfaces combined with the various "glue-ware" required to make the products work within their environment also preclude the open and standard interfaces needed to share that same information seamlessly with any other organization within the DoD/IC – much less with one outside of the DoD/IC Enterprise. The DoD and IC must work closely with the vendor community to identify incentives (financial, regulatory, *etc.*) to establish a commonly accepted access control framework and open the interfaces needed for interoperability.

Objective 4—Establish Government/Vendor/Academia Partnerships for the Research and Development of New and Enhanced Authorization Capabilities

The establishment of government, vendor, and academic partnerships is vital for achieving the specific technology goals of the DoD and IC for enterprise-wide solutions in authorization and access management. The DoD and IC typically lag behind the global IT market in technology maturation and adoption. To truly influence the authorization capabilities, the DoD and IC must engage at the beginning of the technology maturity curve and participate in requirements generation and the research and development needed to produce its specialized capabilities.

In an effort to buy down the risk inherent in research and development (R&D), the DoD and IC should identify select vendor and academic organizations with which to partner for the purpose of developing enhanced enterprise authorization and access control capabilities. These types of partnerships have proven successful in the past. An example of one successful partnership is the Trusted Computing Group (TCG). The TCG develops standards and publishes specifications for security technologies intended to combat the threat of software attack. Trusted Computing Technologies include the Trusted Platform Module (TPM), Trusted Network Connect (TNC), and the Trusted Computing Software Stack (TSS). As the need increases for commercial-off-the-shelf (COTS) products to be the practical solution for protecting certain segments of classified information, DoD/IC can use products that adhere to the specifications of the TCG.

It is important to understand that equal proportions of research and technology development within the four major components of authorization are needed for advancement of the overall authorization service capability.

- **Attribute Management** is the process of managing attributes about the consumer and the consumer's environment. A consumer is anything or anyone that is trying to access a resource. A consumer can be a user, machine, or service. Consumer, identity, subject, and environment attributes require a common syntax, schema, and allowable values. They might be used to make decisions about whether the consumer is authorized to access a resource. Attribute

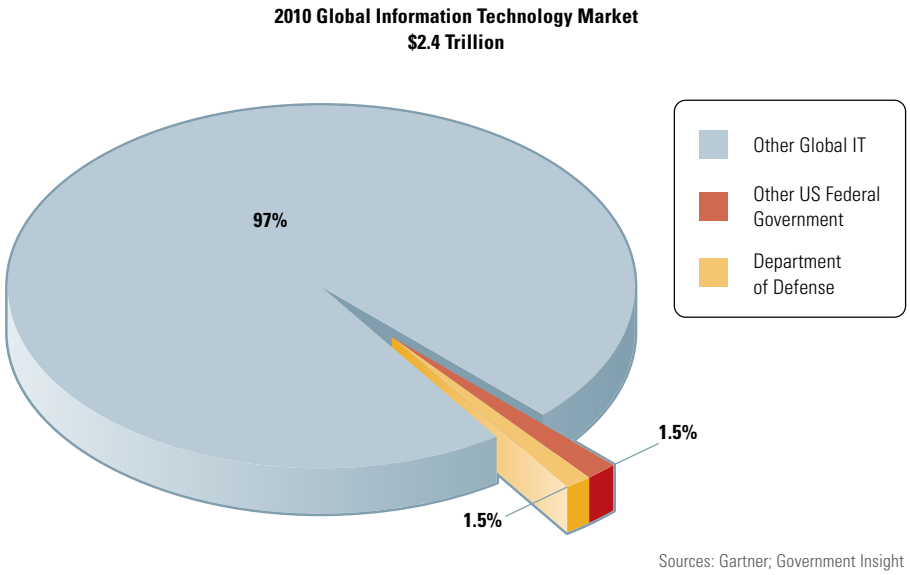


Figure 2 Worldwide IT spending in 2010

stores need clearly defined source authorities and accessible and open interfaces for interaction with access control solutions throughout the enterprise.

- **Metadata Management** deals with managing information about the resource. A resource is any data or service that a consumer requests. Metadata is data about the resource. Metadata has the same needs as other attributes and may be used to add labels to data and services that could be used to render access decisions. While much work has gone into defining metadata concepts, very little has been done to implement or enforce metadata population for the billions of pieces of data under DoD/IC control.
- **Digital Policy Management** is the management of the digital access control policies that are created based on written policies. Digital policies are written to specify what consumers are allowed to access, based on the metadata of the resource, the attributes of the consumer requesting access, and the current environmental context. While this may be the most important aspect of authorization, there has been little progress in developing digital policy capabilities that are exportable or scalable to a large, diverse enterprise.
- **Access Management** is the process of granting or denying access based on the evaluation of the consumer and resource attributes against the digital policy. Again, these solutions tend to be proprietary in nature and work only within a vendor application or as part of a single vendor's enterprise solution. The DoD and IC would benefit the most by opening the decision and enforcement interfaces, for example, allowing multiple vendor policy enforcement products to work with a single enterprise policy decision service.

Source: Gartner, As of September 2009

Figure 3 Mapping of state-of-the-art vendor solutions

Gartner's Magic Quadrants, demonstrated in Figure 3, and MarketScopes provide useful insight into the state-of-the-art vendor solutions available and may help point the DoD and IC in the right direction for future partnerships. [3] One note of caution, however, the Gartner analysis evaluates capabilities in terms of the global set of requirements and is not always going to point to solutions that match the specific and sometimes unique needs of the DoD and IC. While partnership requires a level of risk and commitment of resources by the DoD and IC, the return on investment is a voice at the table when new concepts and technologies emerge. Enhancements that may be applied to the broader global market can emerge, shaped by the specialized, but robust, requirements of the DoD and IC.

Objective 5 – Establish Forums and Outreach Mechanisms for Communicating Evolving Government Requirements and Forecasting Vendor Innovation

Finally, for a commercial engagement strategy to be successful, a well-defined set of outreach mechanisms and forums for sharing concepts, requirements, and trends is needed. A coordinated and enforced communications plan can provide the DoD and IC leadership the opportunity to communicate government needs while aligning enterprise guidance to the trends of the future. Conference events like the DoD's Information Assurance Symposium, the DoD Identity and Protection Management Conference, the DoD/IC Intelligence Information System (DoDIIS) conference, and outreach efforts by the AASC provide an opportunity for the exchange of information needed. Publishing an outreach plan ensures that the goals and objectives of this information exchange are well-understood and that communication can flow unhindered throughout the partnership.

Summary

It is imperative that the DoD and IC not be deterred from realizing the ideal of a robust secure information sharing environment – getting vital information and services only to those who need it, only when they need it, and only for the purposes for which they are authorized. The government must engage and partner with the commercial vendors and standards bodies to work in collaboration and drive the implementation of authorization services through partnership, shared risk, and shared opportunity. With a holistic, actionable, and well-governed approach to achieving these objectives, the DoD and IC will be better prepared for the challenges that lie ahead. ■

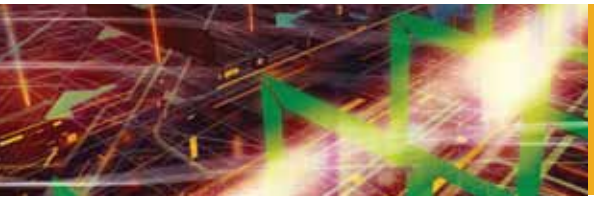
About the Authors

Art Friedman, CISSP | has 32 years of information technology and cybersecurity experience and is a senior strategist for DoD responsible for developing policy and strategy for Identity and Access Management. His education includes an undergraduate degree in mathematics and graduate degrees in business administration and strategic studies. He is a Certified Information Systems Security Professional and a member of (ISC)² Government Advisory Board for Cybersecurity. He serves on several working groups, including the Committee for National Security Systems and the Federal Identity, Credential, and Access Management subcommittee. He can be contacted at *iatac@dtic.com*.

Adam Schnitzer, PMP | currently leads numerous efforts supporting the development of enterprise security strategy, policy, and architecture for DoD. Throughout his career, he served as a surface warfare officer in the U.S. Navy; an instructor at the U.S. Naval Academy; a Command, Control, Communications and Intelligence systems engineer; and an information security professional. Mr. Schnitzer has an undergraduate degree in systems engineering from the U.S. Naval Academy and a graduate degree in national security and strategic studies from the U.S. Naval War College. He is a Project Management Professional and holds a CompTIA Security+ certification. He can be contacted at *iatac@dtic.com*.

References

1. *www.cert.org/archive/pdf/ecrimesummary10.pdf*
2. DOD/IC Federated ABAC Symposium Summary Report. 15 September 2010.
3. *http://www.gartner.com/it/page.jsp?id=1419513*
4. *http://www.nextgov.com/nextgov/ng_20100112_7868.php*



Letter to the Editor

Q ***I think employees in my organization should be able to access Facebook, LinkedIn, and other social media outlets during the work day. What policies or procedures should my organization put in place to protect my organization's information and reputation?***

A An organization can allow its employees to use social media outlets like Facebook and LinkedIn by developing clear, robust information protection and Internet usage policies, implementing an effective monitoring system, and enforcing its policies.

Organizations regularly implement three kinds of information protection policies:

- Employees sign a policy stating that they will not compromise proprietary, sensitive, or classified information.
- Employees sign a policy outlining what constitutes appropriate Internet usage.
- Employees sign a policy stating they understand that the organization monitors Internet usage.

By implementing an effective monitoring system that complements these policies, organizations can reliably identify individuals who are using the Internet inappropriately or in ways that are clearly outside the boundaries that the organization defines. Once the organization identifies one such user, leadership must then take the appropriate punitive actions.

With these types of policies and an effective monitoring system in place, organizations can allow their employees to continue using social media outlets in ways that do not put an organization's information or reputation at too high a risk. ■

Preparing for Incident Response Using the Zachman Framework

by Joanna DeFranco and Phillip Laplante

Most major enterprises, well aware of the cyber threats to their critical assets, maintain a significant focus on both digital forensic investigation and incident response techniques to ensure the authenticity of the data collected if such an incident occurs. But as in firing a weapon, "Aim, Fire" is not enough – the weapon should be "Ready" too.

In the area of digital security, the focus has been two-fold: Incident Response (IR), where computer security incidents are detected and contained; and digital forensics (DF),where the evidence for e-discovery (pre-trial phase where electronic evidence is requested) is obtained and validated. Often pre-incident preparation is thought to be part of the IR process. A successful pre-incident preparation process, however, must have its own focus to reduce the cost and possibility of the DF process, in particular, by ensuring that policies are followed and the data collected is valid evidence that can be presented in a court of law.

Preparation is an important step in ensuring a smooth transition to the digital forensic investigative process and increasing the chances of an effective investigation. This article introduces a framework that rigorously addresses how a company can prepare their infrastructure and protect critical data from cyber threats or at least be in a position to perform an effective digital forensic investigation if an incident does occur. The proposed framework is derived from the Zachman enterprise architecture. [1]

The Zachman Framework

The widely-used framework developed by John Zachman in 1987 (Figure 1) provides a way to rationalize architectural concepts and facilitate communication among the designers of complex information systems. The Zachman Framework can be adapted to model a variety of complex systems.

The six dimensions shown as rows in the framework in Figure 1 represent stakeholder perspectives of a complex system. Essentially, the framework lays out the architectural model that includes each stakeholder, creating a complete view of that system. Zachman's main goal is to emphasize the fact that design is not just about the system itself; it is an enterprise issue.

The columns in the framework are a meta-model that answers the questions what, how, where, who, when and why to describe the enterprise. The "what" describes an inventory of assets. The "how" describes how the transformation of the enterprise will occur. The "where" describes the capacity of the enterprise to store and transport. The "who" describes management of the work performance. The "when" describes the cycle times in the enterprise. The "why" describes a way to manage the enterprise objectives.

The only reported application of the Zachman Framework to digital forensics is Leong's (2006) FORZA model. [2] In this case, Leong used Zachman to define eight roles and responsibilities in a digital forensic investigation using a set of interrogative questions. While Leong's model provides a rigorous approach to post-incident data collection, it does not address the issue of preparation. Mandia, Prosise, and Pepe (2003), a highly cited resource in the area of incident response, recommends six areas for pre-incident preparation: identifying risk, preparing hosts, preparing networks, establishing policies/procedures, creating a response toolkit, and creating a team to handle incidents. [3]

We propose the addition of a new dimension: training. We model these seven areas coupled with several special publications of the National Institute of Standards and Technology (NIST) and other resources using Zachman's framework. This new framework provides a way to analyze the vulnerabilities, provides suggestions for security and education, and presents a plan for overall protection of enterprise resources, data, and information.

In the case of pre-incident preparation, these seven abstraction layers can be derived by analyzing the package diagram shown in Figure 2.

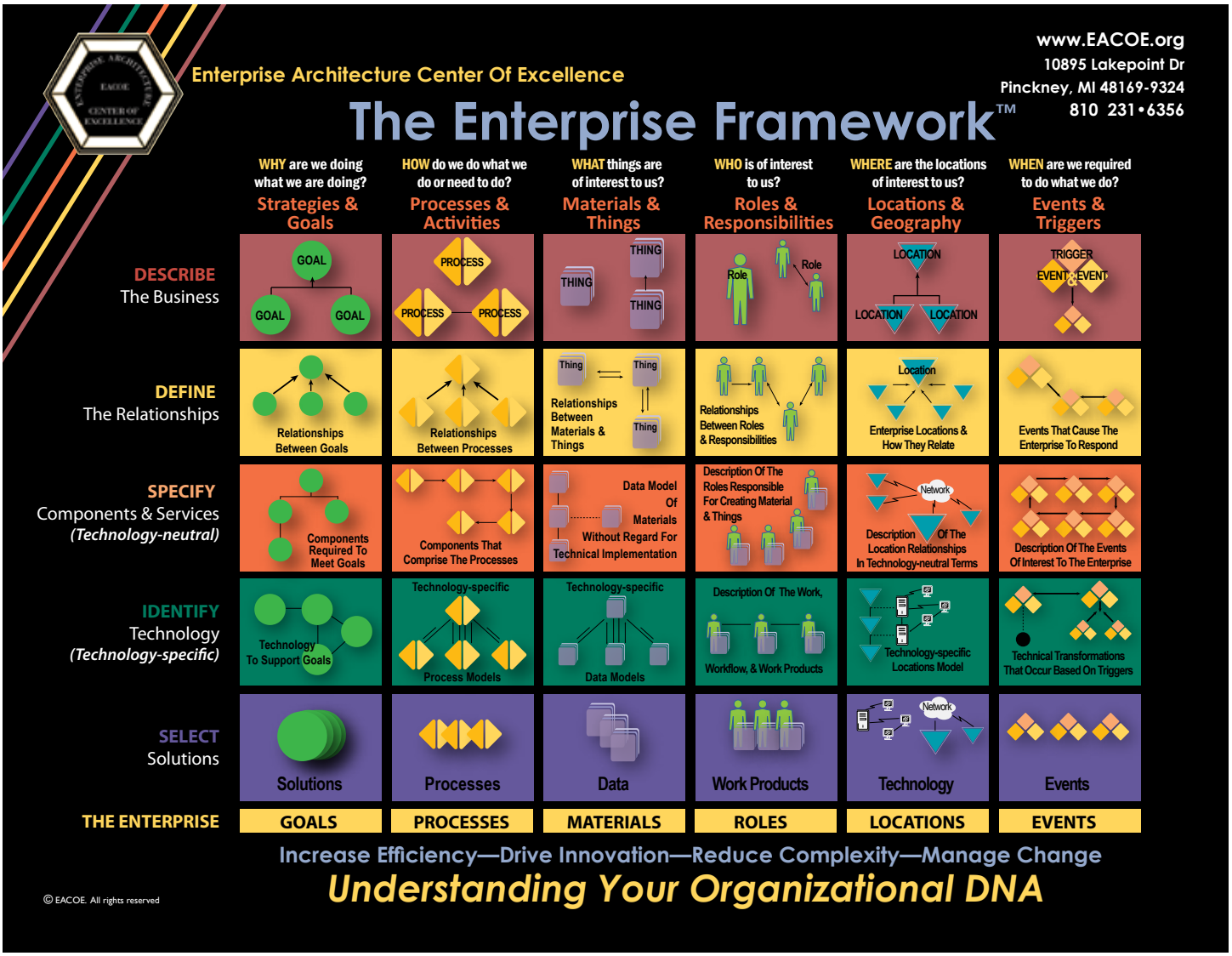


Figure 1 The Zachman Framework (adaptation for incident response preparation)

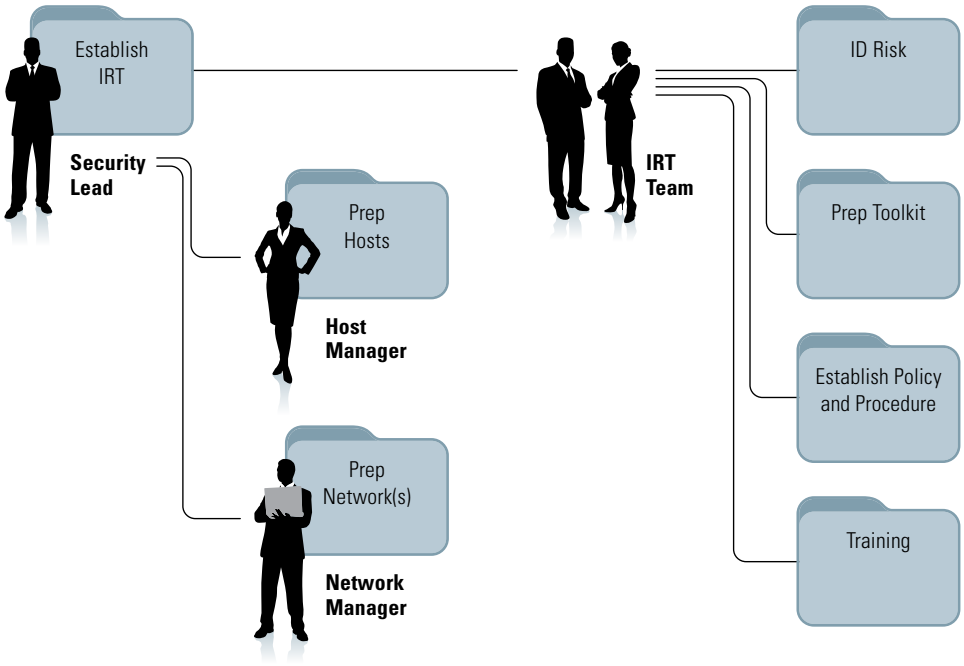


Figure 2 Package diagram depicting seven areas critical to IR and DF preparation

Table 1 illustrates the areas that were adapted by applying the Zachman Framework as well as the factors of interest to effectively prepare for an incident.

Identifying Risk

An effective approach to improving the security posture and preventing incidents is to conduct periodic risk assessments of systems and applications. [3] Assessing risk is clearly the first step in improving a company's security posture. Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. [5]

Because of the dynamic nature of the threat space, it is impossible to determine each vulnerability in a network; however, by determining and addressing known vulnerabilities, the enterprise can be prepared both offensively and defensively.

Which parts of the system need to be secured? What are the critical assets? Who has access to mission critical information/data? Where are the critical assets located?

Critical assets may pertain to confidential customer or company data, critical plans, private individual data, or even the corporate reputation – anything that, if lost, would be extremely harmful to the company's future is considered a risk. Although large networks are vulnerable to hackers, the defenders must worry about malware located everywhere on the Internet, not just external threats to critical assets. In addition, the threats faced by most organizations now focus on internal users. Those users present a risk because of the privileged access to confidential information and critical applications.

When creating a network topology, security personnel can address where critical assets are located. Re-evaluate risk any time a change in network or personnel occurs.

Security personnel must evaluate risks as often as possible and definitely if there is a change in the network or personnel. For example, vulnerability risk evaluation should be run weekly for optimum security and monthly as a best practice. [6]

Preparing Individual Hosts

Disable unnecessary services and configure logging capability of host

NIST recommends several important practices for securing a host, such as limiting user privileges, evaluating default settings and passwords, displaying warning banners for unauthorized use, and enabling logging of significant security related events. [7]

Update application software with any and all patches

Many cyber attacks are directed at heavily-used applications such as word processing or reader applications. Patch alerts targeting users are often ignored. Installing security patches can avoid some of the malicious code that, when installed on a host machine, can spread spam, steal data, or take control of the host. NIST (2004) suggests organizations should implement a patch management program to assist system administrators in identifying, acquiring, testing, and deploying patches. In addition, archiving known vulnerabilities, patches, or resolutions of past problems is a "best practice." [8]

Which files are critical and need a cryptographic checksum recorded? What data is critical that should be backed up and secured? Schedule backups and perform checksum updates when changes occur.

A cryptographic checksum is a hash value produced by running an algorithm on a particular file. Essentially, all bits of data in a particular document or file are added up and a number or hash value is created. This hash value is compared to the hash value generated from the same file on another person's computer or at a previous time on the same computer. Preparation should include determining which files are critical and need some form of authentication signature, such

as a checksum. These values must be backed up and secured along with files. If updates to these critical files occur, a new checksum must be produced.

Who leads the host-based security effort? Where are the host computers located? Who should be educated about host-based security? Who has access to the hosts?

Whoever leads the host-based security effort also must determine and document where the host computers are located and who has access to them. The host-based security lead should also facilitate an education program for host-based security.

Preparing a Network

Encrypt network traffic

All data traveling across a network should be encrypted. For example, e-mail should have content and all attachments encrypted to ensure their integrity. Encrypted e-mails should be stored on multiple servers, included on backups, and inspected by firewalls. Traffic sniffers should also monitor where these e-mails might be stored or travel.

Vulnerability management

Nearly all incidents involving vulnerability exploits can be avoided [9]. Generally, vulnerability scans are performed on the system to determine where it is weak (*e.g.,* any open ports on the firewall expose the system to the outside world). Mobile devices such as USB drives and phones also present a risk. Security personnel should test applications, since hackers now exploit them, as well as the host operating system.

Internal risks

In addition to external risks, companies must be concerned with internal breaches to their networks. Applications to monitor sensitive data as well as specific user status exist already to aid this effort. It is also important to identify which groups of users on the network have access to what types of information. [10]

Network synchronization

With respect to forensic investigations, timing is important. In a digital investigation, having the networks in sync helps determine when incidents occurred. Many organizations use a publicly available time server, or they install one behind the firewall. One downside of a public timeserver is that it leaves a hole in the firewall, though, a private time server is expensive. When using a cloud configuration, synchronized time becomes even more imperative. [11] The forensics performed on a cloud configuration are easier to defend if the time stamps from the

Layers	Factors
Identifying Risks	▸ Determine which parts of system need to be secured—what are the critical assets? (What) ▸ Re-evaluate risk anytime a change in network, personnel occurs (When) ▸ Determine/document location of critical assets (Where) ▸ Determine who has access to mission critical information/data (Who)
Preparing individual hosts (the system that contains the data)	▸ Determine which data is critical and should be backed up and secured (What) ▸ Configure logging capability of host (What) ▸ Update application software with any and all patches (What) ▸ Disable unnecessary services (What) ▸ Schedule backups and perform checksum updates when changes occur (When) ▸ Determine/document where the host computers are located (Where) ▸ Educate users on host based security (Who)
Preparing the network	▸ Document the network architecture and topology (What) ▸ Install Intrusion Protection Systems (What) ▸ Install firewalls, encrypt network traffic, require authentication (What) ▸ Synchronize network (What) ▸ Determine internal risk to network (What) ▸ Vulnerability Management (What)
Establishing appropriate policies and procedures	▸ Develop an Acceptable Use Policy (AUP) (What) ▸ Update the AUP when necessary (When) ▸ Enforce the AUP (Who)
Creating/preparing response tools kit	▸ Acquire necessary hardware to respond to incidents (What) ▸ Acquire necessary software to respond to incidents (What) ▸ Acquire necessary documentation to respond to incidents (What)
Establishing an incident response team	▸ Confirm or dispel whether an incident actually occurred (What) ▸ Establish 24/7 hotlines (What) ▸ Have set timelines for communication with outside parties regarding incidents (When) ▸ Establish process for Incident Response (How) ▸ Conduct investigation, maintain the chain-of-custody, train response team (Who)
Training	▸ Educate users on the proper use of network and applications (Who) ▸ Develop and use lessons learned, penetration testing and live testing (How)

Table 1 Pre-incident preparation model

client-side log files match the time stamps on the provider-side log files.

Install intrusion protection systems, install firewalls, require authentication

The network perimeter must have a configuration that denies activities not expressly permitted. Requiring authentication and installing firewalls and intrusion protection systems should secure network connection points to the organization. [12]

Document the network architecture and topology

A documented network topology assists in determining all affected systems and servers when an incident occurs. An effective way to document the topology is to use a wiki and blogs or bulletin boards to notify administrators of any changes. [13] It is important that the network map resides in a secure location. Some other resources of information that should be included are commonly used ports, operating system documentation, baselines of network and application activity, and hashes of critical files. [14]

Establishing Appropriate Policies and Procedures

Develop an acceptable use policy (AUP)

An AUP is a document containing an extensive set of rules that restrict how the network may be used. An AUP should also outline the policy to prevent malware from the outside, scanning e-mail file attachments, and forbid sending or receiving .exe files, restrict the use of unnecessary software that may be used to transfer malware, restrict removable media, and similar preventive measures. [15] A company can reduce the risk of litigation by publishing and maintaining corporate policies that outline the acceptable use of company resources.

After the AUP is created and available, it must be updated and enforced. The incident response team must choose an "enforcer" of the AUP.

Creating and Preparing a Response Toolkit

Acquire necessary software and hardware to respond to incidents

Carlton and Worthley (2009) collected data from computer forensic examiners and attorneys with computer forensic experience and developed a consensus set of response tasks. For example, they recommend that it is important to wipe and verify target disk drives. Their results also showed agreement on the following tasks: "ensure equipment is fully functional;" "test forensic software tools;" and "ensure that all necessary hardware connectors and adapters are fully stocked." [16] Clearly, these tasks should be performed before an incident occurs.

Acquire necessary documentation to respond to incidents

Implementers of these recommendations must standardize documentation to ensure that all necessary items are recorded. Key areas for documentation include: how the evidence was obtained, all actions taken, and the location and details of the chain of custody. [17] Ten out of the top 26 data acquisition tasks resulting from Carlton and Worthley's work mention these key areas of documentation of specific portions of an investigation.

Establishing an Incident Response Team

Training the response team

A properly trained team is as important as having a secure network. A well-trained team increases the chances of the data validity upon collection. In general, the response team provides technical assistance (analyzing compromised system), conducts eradication activities (elimination of the cause and effect of incident), and performs the recovery (restore systems and services). [18] Outside training involving certifications is one option to educate a team about procedures, processes, and documentation. A major part of this training should be maintaining the integrity of the evidence. Using the procedures suggested in the Network Working Group RFC 3227 is recommended. [19]

A few other responsibilities for the response team occurring after a possible incident are:

- Confirm or dispel whether an incident occurred ;
- Respond to a security incident using established processes ; and
- Determine who conducts the investigation.

Establish 24/7 hotlines and have set timelines for communication with outside parties regarding incidents

Incidents clearly can occur at any time, therefore, a 24-hour hotline must be available. The response team also requires a communication plan for appropriate stakeholders and the contact information from team members, on-call information for other teams within the organization, incident reporting mechanisms to report suspected incidents, encryption software to be used for communications among team members, and a secure storage facility to keep evidence secure. [20]

Maintain the chain-of-custody

The location of evidence from collection to presentation in court must be traceable so that a court can verify the authenticity of electronic evidence. [21] Items to be documented include:

- Where, when, and by whom the evidence was collected;
- Where, when, and by whom the evidence was handled or analyzed;
- Who had custody during what period of time? How was it stored?; and
- If evidence changed custody, document when and how the transfer of custody occurred. Include all shipping information. [22]

Training

Train the users of the network, host, and applications. Educate users about proper use and malware. Use lessons learned, penetration testing, and live testing

All of the preparation efforts recommended here become futile if the users do not understand their importance. Users should be informed about the appropriate use of networks, hosts, and the applications they use. Training should also include guidance about malware incident prevention. [23] This goal can be accomplished by sharing lessons learned from previous incidents so the stakeholders can see how their actions affect the organization. Training can also be a result of "penetration testing," which is a process that evaluates the security of a network. [24]

Users should know how to contact the response team as well as understand the services they provide. The Network Working Group suggests publishing a clear statement of the policies and procedures of the response team in order for the constituents to understand how to report incidents and what to expect after an incident is reported. [25]

The IT staff also should be trained to maintain the hosts, networks, and applications in accordance with the security standards of the organization. [26] One training option is live testing, for example, simulating a cybersecurity incident, then evaluating the reaction and process of the incident response team. This technique is often used in educational settings.

Conclusion

Companies must be prepared for any incident – from an employee misusing company resources – to a hacker creating a denial of service attack on the company web server – to stolen information. The more prepared a company, the better the chances of recovery.

This article shows how the Zachman Framework can be applied as a checklist for addressing preparedness for incident response. As is the hallmark of Zachman-based models, our model can be adapted easily to address the specific needs of any organization. ■

About the Authors

Joanna DeFranco, PhD | is an assistant professor of software engineering at Penn State's Great Valley Graduate Professional Center. Before entering academia, Dr. DeFranco held engineering positions in industry and government, including as a software engineer for Motorola and an electronics engineer for the DoD. She has published articles in academic journals and conference proceedings. Her interests are in the areas of collaborative problem solving, project management, and computer forensics. She can be contacted at *jfd104@psu.edu.*

Phil Laplante, PhD | is professor of software engineering at Penn State's Great Valley Graduate Professional Center. He spent several years as a software engineer and project manager working on avionics (including the space shuttle), CAD, and software test systems. He has authored or edited 26 books and has published more than 150 papers. His interests are in software and systems engineering, project management, and software testing and security. He can be contacted at *plaplante@gv.psu.edu.*

References

1. John A. Zachman (1987). "A Framework for Information Systems Architecture". In: IBM Systems Journal, Vol. 26, no 3, pp. 276-292.
2. NTT Communications White Paper, "8 Elements of Complete Vulnerability Management", September 2009.
3. Mandia, K., Prosise, C., Pepe, M., Incident Response & Computer Forensics, 2nd edition, McGraw-Hill, 2003.
4. Grance, T., Kent, K., Kim, B., "Computer Security Incident Handling Guide", National Institute of Standards and Technology, Special Publication 800-61, 2004, *http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf,* retrieved 1/19/10.
5. Stoneburner, G., Goguen, A., Feringa, A., "Risk Management Guide for Information Technology Systems", July 2002, NIST SP 800-30, *http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf,* retrieved on 1/23/10.
6. *Ibid.*
7. *Ibid.*
8. Brownlee, N., Guttman, E., "Expectations for Computer Security Incident Response", Network Working Group RFC 2350, June 1998.
9. *Ibid.*
10. "Manageable Network Plan", National Security Agency, December 2009.
11. Zimmerman, S., Glavach, D., "Cyber Forensics in the Cloud", IAnewsletter, Volume 14, Number 1, Winter 2011.
12. *Ibid.*
13. *Ibid.*
14. Mell, P., Kent, K., Nusbaum, J., "Guide to Malware Incident Prevention and Handling", Special Publication SP800-83, November 2005.
15. *Ibid.*
16. Carlton, G., Worthley, R., "An Evaluation of Agreement and Conflict Among Computer Forensics Experts", HICSS 2009.
17. *Ibid.*
18. *Ibid.*
19. Brezinski, D., Killalea, T, "Guidelines for Evidence Collection and Archiving", Network Working Group RFC 3227, February 2002.
20. *Ibid.*
21. *Ibid.*
22. *Ibid.*
23. *Ibid.*
24. *Ibid.*
25. *Ibid.*
26. *Ibid.*

Acquisition History and IA Tools—Time for New Thinking?

by Robert Deitz II

Over the last 15 years, the information technology (IT) acquisition process has changed drastically. The government used to use sole source IT contracts, execute mandatory contract vehicles like General Services Administration (GSA), Army DeskTop, *etc.,* and then renew its contract with the same vendor for the duration of the product life cycle. All products, services, and support would be on one contract and use one or a few vendors. IT acquisition consisted of mainframes, mini-computers, and word processing systems where all support, maintenance, hardware, and software came from one company. This process kept the systems current and supported, and there was usually little need for additional in-house resources.

Starting in the mid-1990s, with Y2K on the horizon, Congress passed the Federal Acquisition Reform Act (FARA) and Federal Acquisition Streamlining Act (FASA), significantly changing the government contracting landscape. These acts made GSA and other contracts "non-mandatory" for the first time. The government significantly increased the maximum order limitation for the GSA schedule. Organizations no longer had 1-year contract terms for GSA contracts; therefore, planning and evaluation against GSA schedule products and services became possible. Many contracts moved to 5-year or more contract terms. Organizations developed new indefinite delivery/indefinite quantity (IDIQ) contract vehicles to compete with GSA and agency contracts, such as the National Aeronautics and Space Administration Scientific Engineering Workstation Procurement (SEWP) and National Institutes of Health Electronic Computer Store (ECS).

Within the government, the need arose to pull in multiple outside vendors for multiple year (but theoretically fixed-term) contracts as Y2K approached. There was a steep learning curve during this timeframe, and vendors had to redo more than a few Y2K projects more than once.

A New Acquisition Landscape

After Y2K, outsourcing dominated the acquisition landscape. An organization's computing environment typically included hardware and software from multiple vendors as well as multiple technologies (servers, routers, PCs, *etc.*), all of which needed to be connected to work together. The rules changed, and new procurement policies had to be developed. After 9/11, immediacy became essential, and rapid change occurred in how IT and information assurance (IA) were procured and deployed.

The rapid change caused by various social and political pressures was not easily absorbed into the government business processes. In the 1980s and early 1990s, there had been consistency with one vendor, one contract. Y2K and 9/11 environments now demanded urgency. The new technological environment of networks and distributed systems instead of the mainframes and mini-computers changed information security practices. Practitioners had not put firewalls, intrusion detection systems (IDSs), and anti-virus (AV) software on old systems. As a result, organizations had no historical data or best practices to use as guidelines moving into this new computing environment.

IT in the post 9/11 environment resembled the "Wild Wild West." New manufacturers entered the market at an alarming pace. There was political pressure for outsourcing and the feeling was that private industry knew better than government. No one could rely on past experience, and yet the government had to meet current and future challenges. Everyone was working to avoid another 9/11.

Acquisition Problems Arise Post-9/11

Unfortunately, this environment was conducive to abuse under organizational conflict of interest rules. The government issued many contracts to build networks, Network Operations Centers, Security Operations Centers (SOCs), storage systems, help desks, *etc.,* and it was relatively easy to add additional features under issued

contracts in many instances. Task orders had services, hardware, software, training, and support all under one umbrella, and the temptation to add to contracts that were supposed to be for expertise or services was too great. In many cases, government customers asked contractors to add what they could to existing contracts to avoid issuing new contracts. Large system integrators purchased companies that focused primarily on selling only IT products during this timeframe because of the demand in the market. Service system integrators became the biggest sellers of products under the GSA schedule, and dollars were freely available to increase contract sizes. Large contracts still dominate the federal IT arena today.

Promoting Competition

Many federal agencies depend on large contracts for basic needs; however, in many cases "add-ons" have moved to open procurement and open bidding for every new and renewal purchase, promoting competition, small business participation, and open government. The GSA eBuy or SEWP Web sites are inundated with procurements for monitors, printers, desktop software, *etc.* They are also a primary site for IA tools and renewals since these tools have developed over the years as software add-ons (*e.g.,* anti-spam, IDS, *etc.*); the key question now is: *is this the right method for procuring and supporting IA solutions?*

In today's acquisition environment, we have good support for basic IT hardware and software. You can add Dell, HP, or IBM solutions to an environment, and they work together. Times have changed from a technology standpoint, though, in the case of IA tools. Today's environment requires interconnectivity of IA technologies. In an environment where information security solutions do not talk to each other, security breaches will occur. The failures of 9/11 demonstrated that interconnectivity is paramount. Do we have the right past experience to build on our IA acquisition and deployment skills?

The Future of IA Acquisition—Applying Lessons Learned

The procurement of current IA tools often occurs in a piecemeal fashion through separate competitive bids. There may be written requirements that demand interconnectivity, but in an open procurement process, the government user depends on truthful and knowledgeable responses from the vendor. In the case of many requests for information (RFIs) or requests for proposals, vendors who respond have never met or been on site at the requesting agency. Would you have a surgeon whom you have never met perform surgery?

Many IA tools today are procured *via* low bids from vendors that have never done business with a particular agency. Even with the best intentions, it is not possible to know the background, unique requirements, or special systems installed at a large enterprise. Instead, government organizations hope that the solution fits seamlessly and in harmony with its existing IA tools.

So what parameters do we use to deploy an integrated, tested, survivable IA security platform? We have to live under certain guidelines such as the Federal Acquisition Regulations (FAR), which outlines organizational conflicts of interest (OCI) (FAR Sect 905.4). Many companies have been exposed for OCI non-compliance in the past. From a fair and open procurement standpoint, these cases have had a positive impact. For example, if a systems integrator has a full staff of Check Point, Cisco, McAfee, and similar certified engineers, and a government customer tasks them with evaluating new solutions, what solutions should one expect they will recommend? In the IA world, new and effective solutions often come from new and previously unknown vendors. As long as those vendors comply with Department of Defense requirements (*e.g.,* National Information Assurance Partnership certification, Internet Protocol version 6 compliance, and Federal Information Processing Standards certification) by actual

installation and testing rather than RFI responses where the information may or may not be accurate, they should be considered. It is essential to trust but verify the IA tools critical to an organization's cybersecurity.

It is time to reconsider how IA is sourced in the government community. Today, some IA projects reside predominantly in the civilian sector, such as the U.S. Department of Agriculture's IT Security Tools Blanket Purchase Agreement (BPA) or the Department of Homeland Security Eagle and First Source IDIQ contracts. These contract vehicles allow for direct contact between the government end user and the security tools solutions provider. These contracts de-emphasize interaction with the manufacturer, however, who in many cases does not know other manufacturers' capabilities. It may be time to instead engage the experienced security/IA tools specialist, the independent specialist with no outside interest or conflicts, the government, and IT infrastructure solution providers together to acquire and operate a fully integrated and tested IA platform. By engaging these key stakeholders, perhaps we can finally master effective IA acquisition. ■

About the Author

Robert Deitz II | is Founder and CEO of Government Technology Solutions. He has 32 years of experience in IT with particular expertise in security practices, technology evolution, and security/IA tools development. Mr. Deitz also has a strong background in government contracts with many accomplishments in GSA, BPA, Basic Ordering Agreement, and various state contract efforts. He can be contacted at *iatac@dtic.com.*

DoDTechipedia Happenings

by Ryan Dickson

DoDTechipedia has quickly become one of the premiere collaborative information sharing resources within the Department of Defense (DoD). With more than 33,579 registered Defense Technical Information Center (DTIC) account users and over 889,772 page views, DoDTechipedia provides visitors with in-depth analysis and research on topics ranging from biometrics to secure systems development. DoDTechipedia focuses on enhancing collaboration across government agencies while also serving as a central point for sharing relevant information assurance (IA) breakthroughs and events across the DoD community.

The "News and Events" section, one of DoDTechipedia's most expansive content categories, hosts a comprehensive archive of significant research and development events across 25 knowledge centers. Areas of focus include intelligence, homeland security, military, and defense, among many others. Users add content to the "Information Technology and Cyber Security" domain almost daily. This domain has provided IA professionals with timely access to breakthrough developments and technologies during the last 3 years. By administering a collaborative environment such as DoDTechipedia, the DTIC contributes to President Barack Obama's goal to create an empowered IA workforce in addition to harmonizing significant research efforts across the DoD.

To learn more about DoDTechipedia or to contribute research from your organization, visit *http://www.dtic.mil*. Please note that a DTIC account is required for access. New users can register for accounts at *http://www.dtic.mil/dtic/registration.* ■

University of Tulsa

by Angela Orebaugh

The University of Tulsa (TU) was founded in 1894 by the Presbyterian Church in Tulsa, OK. It is a private, accredited, coeducational university with a variety of programs across 50 undergraduate, 35 graduate, and 10 doctoral degrees. Enrollment currently consists of over 3,000 undergraduate and over 1,000 graduate and law students. [1] TU has over a decade of experience in information security research and education and is known as a leading school within cybersecurity. It is also designated as a National Security Agency (NSA) Center of Academic Excellence (CAE) in Information Assurance Education and an NSA CAE in Information Assurance Research.

In 1996, TU established the Institute for Information Security (iSec), a multidisciplinary cybersecurity program that leverages concepts from computer science, electrical engineering, mechanical engineering, business, and law. The core curriculum for both undergraduate and graduate degrees includes computer science courses from the Department of Mathematical and Computer Sciences.

iSec offers certificate programs in information security for all six federal information security standards endorsed by the Committee on National Security Systems (CNSS):

1. **Information Security Personnel**—NSTSSI 4011
2. **Senior System Manager**—CNSSI 4012
3. **System Administrator**—CNSSI 4013A
4. **Information System Security Officer**—CNSSI 4014A
5. **System Certifier**—NSTSSI 4015
6. **Risk Analyst**—CNSSI 4016A.

iSec offers several continuing education options including Certified Information Systems Security Professional (CISSP) training and Information Security (INFOSEC) professional certification. TU is Oklahoma's only official International Information Systems Security Certification Consortium affiliate and only official CISSP examination source. As a result, iSec has the ability to assist security professionals and practitioners in obtaining the CISSP, which is the "gold standard" in information security certification. iSec also offers a 15-credit-hour INFOSEC certification designed for the working professional. These courses are offered in 3-hour blocks, 2 nights a week for 8 weeks and meet the requirements of Department of Defense 8570.01-M.

iSec's core research concentrations include critical infrastructure protection, security engineering, enterprise security, and digital forensics. Research is performed closely with two congressionally funded centers: the Memorial Institute for the Prevention of Terrorism in Oklahoma City and the Institute for Security Technology Studies at Dartmouth College. In addition, iSec participates in the Institute for Information Infrastructure Protection Consortium, headquartered at Dartmouth College. iSec is rapidly developing a successful track record in technology commercialization, catalyzed by its industry partnerships. Some of these companies include the following:

- **Avansic Digital Forensics Professionals**—*www.avansic.com*
- **Meketrex Technologies**—*www.meketrex.com*
- **True Digital Security**—*www.truedigitalsecurity.com.* [2] ■

References

1. *http://www.utulsa.edu/about-TU/TUFactSheet.aspx*
2. *http://isec.utulsa.edu/*

Background Checks for Trusted Personnel

by Chris Silva

Within the information security space and with an increase in unified governance among organizations, it is not uncommon to have to examine the human side of security policy. A question that is raised quite often is how to establish credentialled personnel around access to trusted information and, specifically, how to effectively conduct background checks on these individuals.

This article, part one in a series about establishing credentials for individuals with access to trusted information, will focus on establishing the appropriate level of access to information. While many in the government sector have roles enforced on them by virtue of federal information protection standards, internal policies may need to be established, edited, or updated to provide consistency in terms of access to information.

What constitutes a position of trust? Most organizations that IANS investigated defined a "position of trust" as a role within a company that requires access to sensitive or critical business information, from personally identifiable information (PII) to National Provider Identifier information, including Payment Card Industry subject information, bank account information, and social security numbers. In addition to this sensitive information, other types can include intellectual property to corporate secrets, physical access to sensitive locations, equipment, or legally controlled materials and information acquired through partnership with the federal entities that is classified in some manner.

The U.S. Federal Sentencing Guidelines state that "'public or private trust' refers to a position characterized by professional or managerial discretion. Persons holding such positions ordinarily are subject to significantly less supervision than employees whose responsibilities are primarily non-discretionary in nature. For this adjustment to apply, the position of public or private trust must have contributed in some significant way to facilitating the commission or concealment of the offense (*e.g.,* by making the detection of the offense or the defendant's responsibility for the offense more difficult). This adjustment, for example, applies in the case of an embezzlement of a client's funds by an attorney serving as a guardian, a bank executive's fraudulent loan scheme, or the criminal sexual abuse of a patient by a physician under the guise of an examination. This adjustment does not apply in the case of an embezzlement or theft by an ordinary bank teller or hotel clerk because such positions are not characterized by the above-described factors." [1]

When establishing levels of access, it is often asked whether all trusted positions need a clearance or if a background check is sufficient. To determine the type of clearance warranted for government and military sectors, Department of Defense (DoD), and other government contractors, organizations follow policy, contract language, and guidance from the government agencies to which they are contracted. Contractor investigations and clearances are performed by the same agencies (Defense Security Service, U.S. Office of Personnel Management, *etc.*) that perform them for government/military employees; federal, state, and local government contractors; and outsourced service providers (*e.g.,* fire fighters, contract prisons, *etc.*).

The following is a partial list of non-government/military (or contractor) positions that might warrant background checks or further clearances:

- **Critical Infrastructure Sectors**—Food production/agribusiness, public health/healthcare, water/water treatment, energy production/refining/storage/distribution, electric and nuclear power, banking/finance, defense industrial base, or national monuments/icons. [2]
- **Other "Sensitive" Industries and Businesses**—Pharmaceuticals, chemical manufacture, biological agent manufacture, private security firms, private investigators, or law firms.

- **Other Sensitive Positions/ Positions of Trust (Regardless of Organization)**—IT/network security, contracts/legal, human resources, facility/industrial security, financial, executives, or members of a board of directors.
- **Organizations/Businesses that Routinely Handle Privacy Information/PII**—Ministers, lawyers, social workers, psychological counselors, *etc.*
- **People Who Work with or Around Children**—Teachers and other school employees, church ministry, staff and volunteers, child care/day care, *etc.*

When is a clearance necessary? In the organizations that IANS interviewed, the only time clearances were needed or sought was if the position required interaction with a federal agency, federal or state law enforcement entity, or the military, and some of the information the individual would need access to was classified above a person's current security level. In addition to standard DoD clearances of Secret and Top Secret, IANS also came across the Department of Energy's Q and L clearances.

Officially, government clearances are needed to access Confidential, Secret, Top Secret, and Sensitive Compartmented Information (SCI) and/or the facilities that handle such information as well as for access to Secret Special Access Programs (SAP). The following are the specific types of investigations involved for government clearances:

- **Confidential and Secret Clearances**—National Agency Check with Local Agency Checks and Credit Check
- **Top Secret, SCI, and SAP Clearances**—Single Scope Background Investigation.

For background checks, the degree to which an individual's background should be examined is related to the sensitivity of the information or access they will have in their position—the more critical the resources, the more an incompetent or unethical employee puts a company at risk.

While many companies IANS examined had difficulties giving us exact details as to which checks were being conducted, we found some excellent resources to help quantify these checks based on job role or position, and the types of checks that should be combined:

- University of Georgia Positions of Trust Matrix indicates which positions of trust require which background checks: *http://www.hr.uga.edu/pot.pdf.*
- Northrop Grumman Electronic Systems indicates minimum background investigation and drug screening standards required for all contract labor/service personnel: *https://oasis.northgrum.com/esss/purch/CMF/P481-F02RevD.dot.*

Once specific personnel to be checked and the means for conducting the check have been established, many organizations inquire about the type of information and scope of the checks others are conducting. In the private sector, prevalent background checks are done on the following records of (potential) employees:

- Credit ratings and history, bankruptcy records
- Criminal, court, and incarceration records
- Terrorist watch list
- Sex offender lists
- Academic records
- Employment references and history, including gaps in employment history and offices/positions of trust held
- Motor vehicle/driving and vehicle registration records
- Character reference checks that include interviews with neighbors, friends, or associates about the character, general reputation, personal characteristics, or mode of living of the subject, (such background checks are termed "investigative consumer reports" in the U.S. Fair Credit Reporting Act)
- Identity, social security number, and address verification (both present and previous addresses)
- Passport validity
- Worker's compensation records
- Medical records.

In addition to various combinations of these checks, background checks for specific industries may look at other records. For example, investigations for the aviation industry will do a Federal Aviation Administration records check that conforms to the Pilot Records Improvement Act of 1996.

In the next article in this series, IANS will cover the cost and potential limitations of checks as well as provide an overview of relevant legislation driving the use of checks inside organizations. ■

About the Author

Chris Silva | is the senior vice president of Research and Service Delivery at IANS. In this role, Mr. Silva runs all daily operations of IANS's syndicated research and custom client advisory activities. Mr. Silva is committed to innovating the IANS research methodology to better serve security professionals. Mr. Silva comes from within the IT research industry and is a veteran of several established research businesses. Mr. Silva served 4 years at Forrester Research, most recently as a senior analyst working to serve Security/Risk and Infrastructure/Operations professionals. Mr. Silva is a graduate of the Isenberg School of Management at the University of Massachusetts. He can be contacted at *iatac@dtic.com.*

References

1. *http://www.ussc.gov/2003guid/3b1_3.htm*
2. Homeland Security Presidential Directive (HSPD)-7.

David Greer

by Angela Orebaugh

This article continues our profile series of members of the Information Assurance Technology Analysis Center (IATAC) Subject Matter Expert (SME) program. This article profiles the SME Mr. David Greer from the University of Tulsa (TU). Mr. Greer is the Executive Director of TU's Institute for Information Security (iSec).

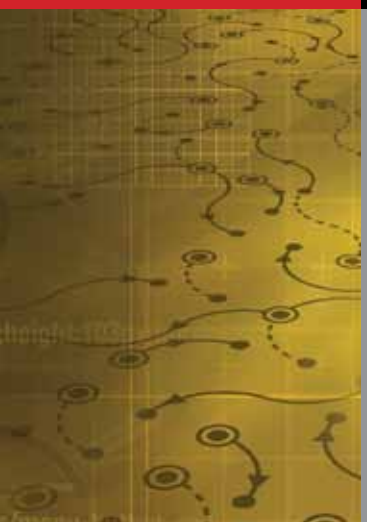
Mr. Greer has over 10 years combined experience as an information security and digital forensics consultant, Cyber Security Education Consortium coordinator, e-learning coordinator, and software compliance specialist. He leverages his expertise to lead iSec in the development, implementation, and supervision of their mission to produce exceptional graduates and technical discoveries in the information security field. He also serves as the liaison between iSec and industry, government, academic partnerships, and alumni. Mr. Greer's duties also extend to seeking research funding for classified and unclassified public and private projects. [1] Mr. Greer serves as an advisor for TU's continuing education and technology commercialization programs and the Oklahoma State University-Okmulgee's cybersecurity program; he is also the Director of Education for the Oklahoma chapter of the Information Systems Security Association.

Mr. Greer spent 5 years as an information security coordinator developing continuing education and e-learning courses in cybersecurity and digital forensics for the Oklahoma Department of Career and Technology Education. Mr. Greer conducts continuing education and instructor training courses in information assurance (IA), secure electronic commerce, network security, enterprise security management, digital forensics, security awareness, information security integration, and cybercrime investigations. He has also designed and built three IA and digital forensics mobile laboratories for use by local, state, and federal law enforcement agencies as well as security professionals.

Mr. Greer earned his Master's Degree in Computer Science and is currently pursuing his Ph.D. from TU. He has filed for several U.S. Patents in the area of digital forensics. Most recently he filed a patent titled "Redaction of Digital Information from an Electronic Device." Mr. Greer is an active Certified Information Systems Security Professional and has received all five federal IA certifications from the Committee on National Security Systems. [2] ■

References

1. *http://isec.utulsa.edu/aboutus/faculty/david-greer/*
2. *http://www.linkedin.com/pub/david-greer/4/533/b7*



7th Annual Information Technology Security Automation Conference

The 7th Annual Information Technology (IT) Security Automation Conference will be held October 31, 2011 through November 2, 2011 in Arlington (Crystal City), VA. This conference will focus on the following topics: Continuous Monitoring, Software Assurance, IT Security Threats, Network Security Automation, and Management and Compliance. The event will also include an exposition showcasing the leading vendors in the security automation industry. For more information on this event, please see *http://scap.nist.gov/events/index.html.*

To learn more about security automation, look for the Fall 2011 edition of the *IAnewsletter,* which will feature a collection of articles on the topic.

Cybersecurity Innovation for the Network Operator Community

by Ross Stapleton-Gray

The Internet is a network of networks, every one managed by operators, and their network operations centers (NOC). NOC operators maintain the integrity and availability of their own networks, and collaborate with other operators to respond to problems.

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has funded cybersecurity research and development (R&D) efforts to provide tools and resources to this global community. This article showcases some of the S&T-sponsored innovations that will allow network operators to respond effectively to problems in the future.

Prefix Checking

The Internet's quilt of independent networks—known formally as Autonomous Systems (AS)—are announced to the rest of the Net community using the Border Gateway Protocol (BGP). BGP announcements describe the networks' connectivity and inform routers where traffic may be sent.

Announcing routing prefixes is critical to the Net's operation but can be a laborious task, and the effects of erroneous or malicious routing announcements can be significant. The notorious February 2008 Pakistani YouTube "hijacking," where an attempt merely to block Pakistani users' access to YouTube unintentionally diverted all YouTube-bound traffic to a Pakistani Internet Service Provider (ISP), was due to a mistaken routing announcement.

An S&T-supported Prefix Checker reduces the expertise required by operators in crafting and submitting routing announcements; the Prefix Checker is designed to provide a basic "sanity check" on submissions.

INOC-DBA

The inter-Network Operations Center dial-by-Autonomous System Number (ASN) (INOC-DBA) is a voice-over-Internet-protocol (VoIP) hotline phone system used by NOC operators to coordinate responses to incidents and issues affecting the Internet.

Each of the autonomous systems that make up a part of the global Internet has a unique ASN, issued by the appropriate regional Internet registry. The IP addresses of traffic originating from a particular network indicate its ASN, and the ASN can then be used on INOC-DBA as if it were the phone number to reach those responsible for that autonomous system.

The INOC-DBA system:

- Lives atop the regular Internet infrastructure, as a logical hotline phone system;
- Makes use of standard VoIP phones; and
- Includes directory services so that one can also look up specific users by name or by organization.

That INOC-DBA runs on the same infrastructure its users are responsible for managing makes it cheap to deploy and operate. On the other hand, that also makes it at risk for denial-of-service attacks on the infrastructure itself. Researchers are investigating ways to make INOC-DBA more survivable.

Supporting communication between all of these widely scattered NOC operators is a critical issue: expertise and individual efforts are still major factors in the Internet's defense. The Net is not a slowly developing and locally focused infrastructure, like a water system, where change is evolutionary. Its speed and interconnectivity allow Internet attacks to be launched from half a world away. This point underscores the importance of linking NOC operators. The basic requirement for INOC-DBA membership is to merely be responsible for running a portion of the global Internet. Any organization assigned an ASN can join, and participation in INOC-DBA does not require that you afford the other participants any greater level of trust, it merely assures you that they are the responsible authorities for their particular portions of the Net.

DHS S&T has sponsored R&D to refine and expand INOC-DBA. Current and planned enhancements include providing multi-party conference bridging, which can in turn support new

applications, such as group voting, and stronger means of authentication.

INOC-DBA's developers are now looking to establish it as a substantial part of the communications and management infrastructure for those who themselves manage the Internet as an increasingly critical, global infrastructure.

PREDICT

DHS S&T sponsors another important effort aimed at providing cybersecurity researchers with real-world data for analysis and testing: the Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT) program.

Rather than an actual physical repository, PREDICT is actually a community. A portal established by S&T serves to coordinate data providers, data hosts, and researchers. Specific PREDICT users might assume any or all of these roles: collecting network traffic, usage data, curating the resulting datasets, and using data to design and test new systems to anticipate potential threats or to understand actual incidents.

PREDICT datasets include data collected in portions of the global Internet that have not been announced as available for routing. Any traffic in these segments ought not to be there, so would be the result of either error or malicious behavior.

Data derived from INOC-DBA VoIP traffic contributes to the PREDICT collection. Future plans for PREDICT datasets include snapshots of Internet topology, exchange point peering information, and cable infrastructure.

DETER

PREDICT data in turn contributes to yet another DHS S&T investment, the DETER testbed (derived from "cyber-Defense Technology Experimental Research"). Initially launched as a joint effort by S&T and the National Science Foundation (NSF), DETER is now maintained by S&T. The aim of DETER is to provide researchers with a secure means to test next-generation cybersecurity technologies within a realistic Internet environment, including against actual malicious code.

Physically, DETER is several clusters totaling several hundred servers, at sites including the University of Southern California (USC) and the University of California at Berkeley. Logically, it can appear to be thousands of configurable hosts, laid out in a network topology that suits a researcher's particular needs. Isolation from the "open Internet" is a critical concern. Researchers would like to be able to subject realistic systems to actual malware without the risk of that malware threatening other systems.

Earlier this year, USC announced that DHS S&T had signed a 5-year $16 million contract to extend and expand DETER with a new project to be called DETECT.

DHS Science and Technology

The Prefix Checker, INOC-DBA, and several dozen other efforts have been sponsored by the DHS S&T Homeland Security Advanced Research Projects Agency (HSARPA) Cyber Security Division (CSD). CSD enables and supports research, development, testing, evaluations, and transition for advanced technologies in cybersecurity and information assurance.

CSD, headed by Dr. Douglas Maughan, is the umbrella under which DHS's cybersecurity R&D activities are coordinated and performed, and it works to create partnerships between government and private industry, the venture capital community, and the research community.

DHS S&T is currently engaged in a Broad Agency Announcement to fund cybersecurity R&D. One of the 14 technical areas in which it is seeking solutions to cybersecurity challenges is "Incidence Response Communities." Even as its past investments are providing tools for those communities, DHS S&T is hoping to better understand the characteristics that distinguish great cybersecurity incidence responders from average technology contributors. DHS S&T's new cybersecurity R&D solicitation encourages use of DETER and of PREDICT datasets as testbed environments for performers.

Using These Services

As DHS S&T prepares to invest more heavily in cybersecurity R&D, many organizations familiar with its efforts are working to put the results of S&T R&D into use.

I encourage *IAnewsletter* readers to actively participate in the advancement of these efforts. Please visit the following sites to see how you can become more involved:

- **To use the Prefix Checker, visit *https://prefix.pch.net/applications/prefix-sanity/*—***(requires* a free user account);
- **To join INOC-DBA, visit *http://www.pch.net/inoc-dba/*—** Use of INOC-DBA requires a validated user account, which merely requires that the requestor be responsible for an AS, and recognized as such by one of the regional Internet registries;
- **DHS PREDICT portal, visit *http://www.predict.org*—**PREDICT is open to U.S. users, including foreign researchers sponsored by U.S. institutions; and
- **DETER and the DETERlab testbed, visit *http://www.isi.edu/deter/*.** ■

About the Author

Ross Stapleton-Gray, Ph.D. | is research program manager at Packet Clearing House, Inc. (PCH), a non-profit research institute dedicated to development and management of the global Internet. Prior to joining PCH, he served as an intelligence analyst for the Central Intelligence Agency, and in information policy positions with the American Petroleum Institute and the University of California Office of the President. He can be contacted at *iatac@dtic.com*.

FREE Products Order Form

Instructions: All IATAC LIMITED DISTRIBUTION reports are distributed through DTIC. If you are not a registered DTIC user, you must do so prior to ordering any IATAC products (unless you are DoD or Government personnel). To register online: *http://www.dtic.mil/dtic/registration.* The *IAnewsletter* is UNLIMITED DISTRIBUTION and may be requested directly from IATAC.

Name _____ DTIC User Code _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

Please check one: ☐ USA ☐ USMC ☐ USN ☐ USAF ☐ DoD ☐ Industry ☐ Academia ☐ Government ☐ Other

Please list the Government program(s)/project(s) that the product(s) will be used to support: _____

_____

LIMITED DISTRIBUTION

IA Tools Reports ☐ **Firewalls** ☐ **Intrusion Detection** ☐ **Vulnerability Analysis** ☐ **Malware**

Critical Review and Technology Assessment (CR/TA) Reports
- ☐ Biometrics (soft copy only)
- ☐ Configuration Management (soft copy only)
- ☐ Defense in Depth (soft copy only)
- ☐ Data Mining (soft copy only)
- ☐ IA Metrics (soft copy only)
- ☐ Network Centric Warfare (soft copy only)
- ☐ Wireless Wide Area Network (WWAN) Security
- ☐ Exploring Biotechnology (soft copy only)
- ☐ Computer Forensics (soft copy only. DTIC user code MUST be supplied before this report is shipped)

State-of-the-Art Reports (SOARs)
- ☐ Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain (DTIC user code must be supplied before this report is shipped)
- ☐ Measuring Cybersecurity and Information Assurance
- ☐ The Insider Threat to Information Systems (DTIC user code must be supplied before this report will be shipped)
- ☐ A Comprehensive Review of Common Needs and Capability Gaps
- ☐ Software Security Assurance
- ☐ IO/IA Visualization Technologies (soft copy only)
- ☐ Modeling & Simulation for IA (soft copy only)
- ☐ Malicious Code (soft copy only)
- ☐ Data Embedding for IA (soft copy only)

UNLIMITED DISTRIBUTION

IAnewsletter hardcopies are available to order. Softcopy back issues are available for download at *http://iac.dtic.mil/iatac/IA_newsletter.html*

Volumes 12	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 13	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 14	☐ No. 1	☐ No. 2	☐ No. 3	

SOFTCOPY DISTRIBUTION

The following are available by e-mail distribution:

- ☐ IADigest
- ☐ Research Update
- ☐ Cyber Events Calendar
- ☐ Technical Inquiries Production Report (TIPR)
- ☐ IA Policy Chart Update

Fax completed form to IATAC at 703/984-0773

IATAC
Information Assurance Technology Analysis Center
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171

Calendar

August

GFIRST 2011
7–12 August 2011
Nashville, TN
http://www.us-cert.gov/GFIRST/

DISA Customer and Industry Forum
15-18 August 2011
Baltimore, MD
http://www.disa.mil/conferences/

LandWarNet
23-25 August 2011
Tampa, FL
http://www.afcea.org/events/landwarnet/11/intro.asp

AFITC 2011
29–31 August 2011
Montgomery, AL
http://www.mc2-afitc.com/

September

Biometric Consortium Conference and Technology Expo
27–29 September 2011
Tampa, FL
http://events.jspargo.com/biometrics11/public/enter.aspx

October

AUSA 2011 Annual Meeting and Exposition
10–12 October 2011
Washington, DC
http://www.ausa.org/meetings/Pages/NationalMeetings.aspx

McAfee FOCUS 11
18-20 October 2011
Las Vegas, NV
http://www.mcafeefocus.com/focus2011/

TechNet International 2011
20-21 October 2011
Heidelberg, Germany
http://www.afcea.org/europe/events/tni/11/foreword.asp

November

CSI 2011 Annual Conference
6-11 November 2011
Washington, DC
http://gocsi.com/events

DTIC 2011 Fall Workshop
7-8 November 2011
Alexandria, VA
http://fbcinc.com/event.aspx?eventid=Q6UJ9A00P6CC

USSTRATCOM Cyber and Space Symposium
15-17 November 2011
Omaha, NE
http://www.afcea.org/events/stratcom/11/introduction.asp