

Enabling Mission Critical Operations Through Mature Implementation

by Nadya Bartol, Eric White, Stephanie Shankles, and Michelle Moss

Operations environments are growing increasingly complex as companies and agencies join the net-centric community, where architecture is collaborative and information access instantaneous and global. Led by the Department of Defense's (DoD) vision of Net-Centric operations and the demands of modern warfare, a community has formed in which warfighters and business and intelligence users can share knowledge on a secure and reliable network anywhere worldwide. [1] The dilemma that weighs heavily on the minds of information technology (IT) managers and technology leaders is how they can support the community's warfighters and still respond consistently, with accuracy and speed, to mitigate the risks their systems face. These risks come not only from their own network but also from others with whom they interface. For example, to provide warfighters access

to real-time information on the ground, their vehicles were networked. With the increased functionality comes increased risk. Now, the enemy capture of a US Army Humvee represents more than simply loss of transportation; it may also be a potential threat to the greater tactical network. The Army vehicle, through its on-board computer, is linked to the Marine Corps' ground network, which is part of the Navy's tactical networks. If that opportunity is exploited, all connecting information and networks share the potential risk. [2]

To mitigate those risks, an increased number of industry leaders are seeking to protect their missions and systems by using a powerful combination of information assurance (IA) management tools and processes that strengthen security of core business operations and help them interact with external organizations seamlessly and securely. These IA tools

center on implementing maturity model principles, coupled with other accepted industry specifications and standards. Organizations implementing these IA tools are improving the responsiveness and robustness of IA operations and are facilitating an increase in their effectiveness, support repeatable execution, and ability to respond to sudden events with confidence. As Figure 1 illustrates, teams are learning that repeatable execution takes the guesswork out of response and frees up time and resources for solving real problems. Operational IA standards and controls are helping leaders move forward and identify other areas that could benefit and improve using the same standards and controls. Defined and well managed activities not only lead to better managed and lower IT costs but also support increased collaboration between the IT and business teams. Organizations are pleased to realize that

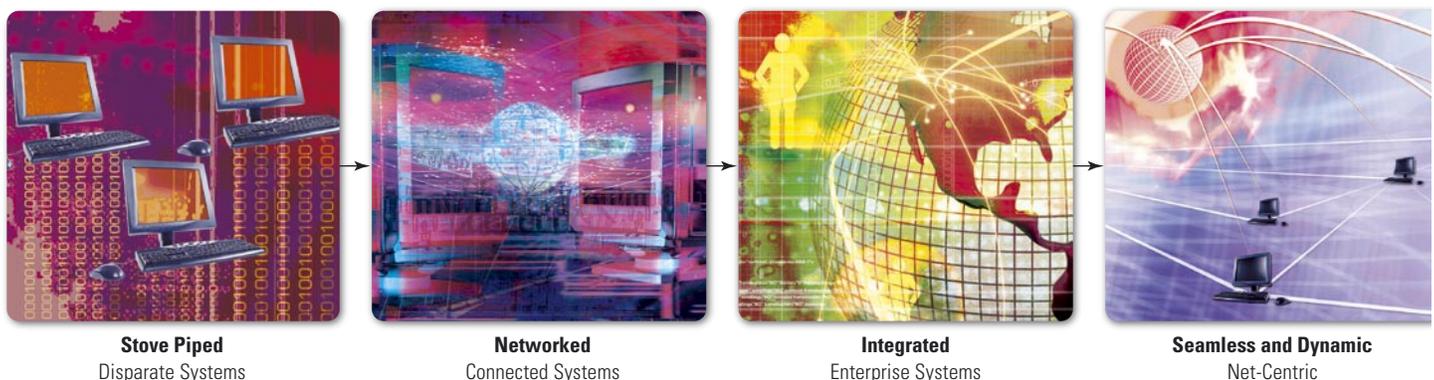


Figure 1 Impacts of Creating an Effective Organization



as they learn to master effectively running their teams and projects using effective standards and controls, they are able to build and manage more reliable systems and handle greater complexity.

The need to work across the IA community to build stronger systems for net-centric operations is apparent. Yet, many organizations struggle with internal divisions operating independently with disparate IA, policies, and operational processes. This means missions are inadequately defined, resources are duplicated, and debates persist over methods for IA implementation, which translates into increased cost and can waste valuable response time. Organizations need to be able to work across functions and respond to threats and challenges to increase success and protect assets. Employing standardized measures and procedures, built into the systems and operations from inception, exponentially decreases the risk and cost incurred because teams can act without guesswork when action is needed.

Protecting and enabling the warfighter in the field means that an organization's core business practices need to be structured, secure, and interoperable. This does not imply bureaucracy; on the contrary, structured, secure, and interoperable processes provide a foundation for making complex decisions timely and effectively, which impacts the number of benefits. Team

members actively participate in creating standards and roles ensuring a relevant structure. Leaders experience a productivity increase because only traceable, authorized work is performed by teams that, by following the defined structure and processes, minimize overlapping efforts. Service quality increases as irregularities decrease, eliminating distractions and allowing team members to focus their energy on work directly relating to the operational goal. Corresponding costs and levels of IT service are better understood, permitting informed business decisions and better relationships between business and IT partners. Built-in continuous improvement processes ensure that business applications operate efficiently throughout the life cycle, making the decision and action repeatable so that responses are complete and reliable. Consequently, complex, critical missions receive the support they need when they need it.

Success Factors

Management commitment and patience are keys to creating an effective organization. Mistakes and setbacks should be expected, along with initial resistance from stakeholders. Preparing unified processes and imparting a streamlined structure constitute a major change; as such, they require team members to fundamentally change the ways of performing the mission, which is

neither easy nor consuming. Leadership must continuously communicate to all stakeholders that improvement is key to success and that the change is inevitable. Leadership must also lead by example in simple tasks such as following new processes and attending training efforts.

As organizations begin to strengthen their core, they realize that processes cannot be improved without a means to measure a desired outcome. Tracking activities and results and turning data into information will free up resources and money, enabling teams to respond to new challenges and maintain acceptable security posture. Measurement of activity allows leaders to view data captures from work efforts and match them with mission objectives. The bidirectionality of the data also helps refine mission objectives by highlighting where the teams' largest impact is being made. Measures provide the data needed to make the right decisions and meet requirements on schedule.

Unified teams operating with clearly defined behaviors and actions experience simplified IT change management. Because they share a common point of reference for internal communications, the right groups understand the information being communicated. Change management produces these benefits because all IT approaches and developments are standardized. Teams can interact and share information efficiently and securely because integration

points and handoffs are well documented and understood, ensuring interoperability and effectiveness in the global environment. Through repeatable actions, performance improvement opportunities are identified, enabling teams to leverage previously defined actions from other teams and apply to and improve their operations. Organizations can respond to additional opportunities because their processes, guides and training, and knowledgeable team members become interchangeable as more teams begin to use similar processes and procedures. Having a strong core also allows measurement to be applied to other project areas for easier tracking and faster results. A strong core throughout the organization enables a structured enterprise view, making it easier to see and maintain various service levels in a complex net-centric environment.

Enabling Tools and Techniques

Various models and tools are available to facilitate increased effectiveness of operations in support of the mission. Governments and industry organization have created standards, frameworks, and maturity models to help organize activities for increased effectiveness (see Figure 2). Although many are focused on technology implementation, they can be easily adopted for increasing effectiveness of operations in support of the mission.

Models are typically composed of processes that are sets of practices performed to achieve a goal. Processes include procedures, methods, tasks, tools, equipment, and people. The quality of a system is governed by the quality of the processes used for developing and maintaining that system. Standards exist for nearly every field of work and are typically documents established by consensus and approved by a recognized body. They provide rules or characteristics for activities and their results. Standards are guidelines and considered voluntary; however, they can become mandatory if they are adopted or referenced by laws or regulations.

The common thread among most of these standards, frameworks, and maturity models is that they mention manage-

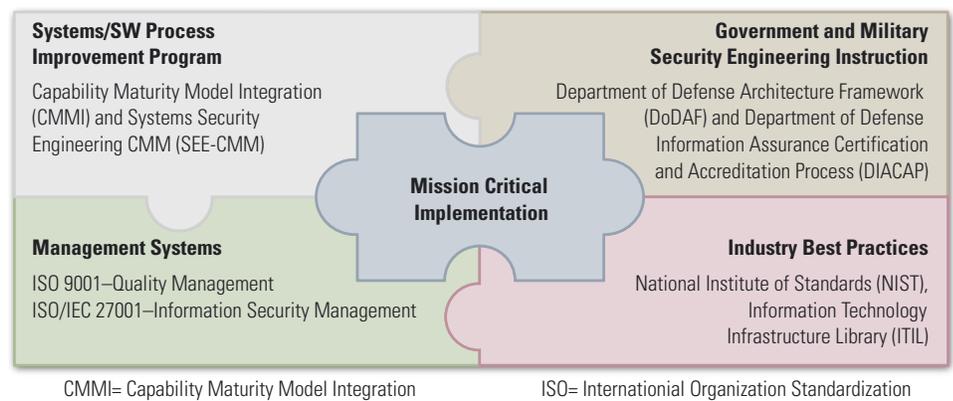


Figure 2 Mission-Critical Implementation

ment commitment, measurement, and change control as key components for successful implementation.

Examples of such models, standards, and frameworks include ISO 90001, *Quality Management System*; ISO/IEC 27001, *Information Security Management System Requirements, Capability Maturity Mode Integration* (CMMI); and ISO/IEC 21827, *System Security Engineering Capability Maturity Model* (SSE CMM), and Information Technology Infrastructure Library (ITIL). The US Government also uses its own series of policies, standards, frameworks, and requirements, such as DoD IA Certification and Accreditation Process (DIACAP), the National Institute for Standards and Technology standards and guidance, DoD Architecture Framework (DoDAF), and Federal Enterprise Architecture (FEA).

Blurring the boundaries between government and industry, caused by increasing interconnectedness and interoperability of networked systems, outsourcing of services, and the fact that more than 85 percent of national critical infrastructure are owned by the industry, necessitates government and industry to ensure that the requirements and the involved domain are interoperable and compatible. Increasingly, government procurements are requiring adherence to government and industry standards, models, and frameworks. By proving compliance with these requirements, vendors can provide a level of assurance that their products and services will withstand

the pressure of the operational environment and will continue supporting the mission in adverse circumstances.

Meeting these standards is often a qualifier for customers to select providers because most mature teams prefer to work with other mature groups. [6] As more organizations realize that they must identify ways for improving their processes and practices, they recognize that working with less standardized organizations wastes resources. That situation effectively requires them to teach the other organization better methods and subjects themselves to greater risks because the less mature group may cut corners or worse and not have necessary IA controls in place to protect their fighters and information.

Any of these methods can be used as a means for provider organizations to evaluate their own behaviors and identify areas of improvement. For example, Lockheed Martin was able to use a combination of methods, including CMM, ISO standards, and a process library, all while achieving their CMMI rating. The team achieved an overall 72-percent increase in productivity from SW-CMM maturity Level 3 as a result of process improvement. [4]

Compliance or Assurance?

Networked systems and organizations must trust each other so that responses are automatic and timely for effective information sharing and to minimize damage and loss when security is

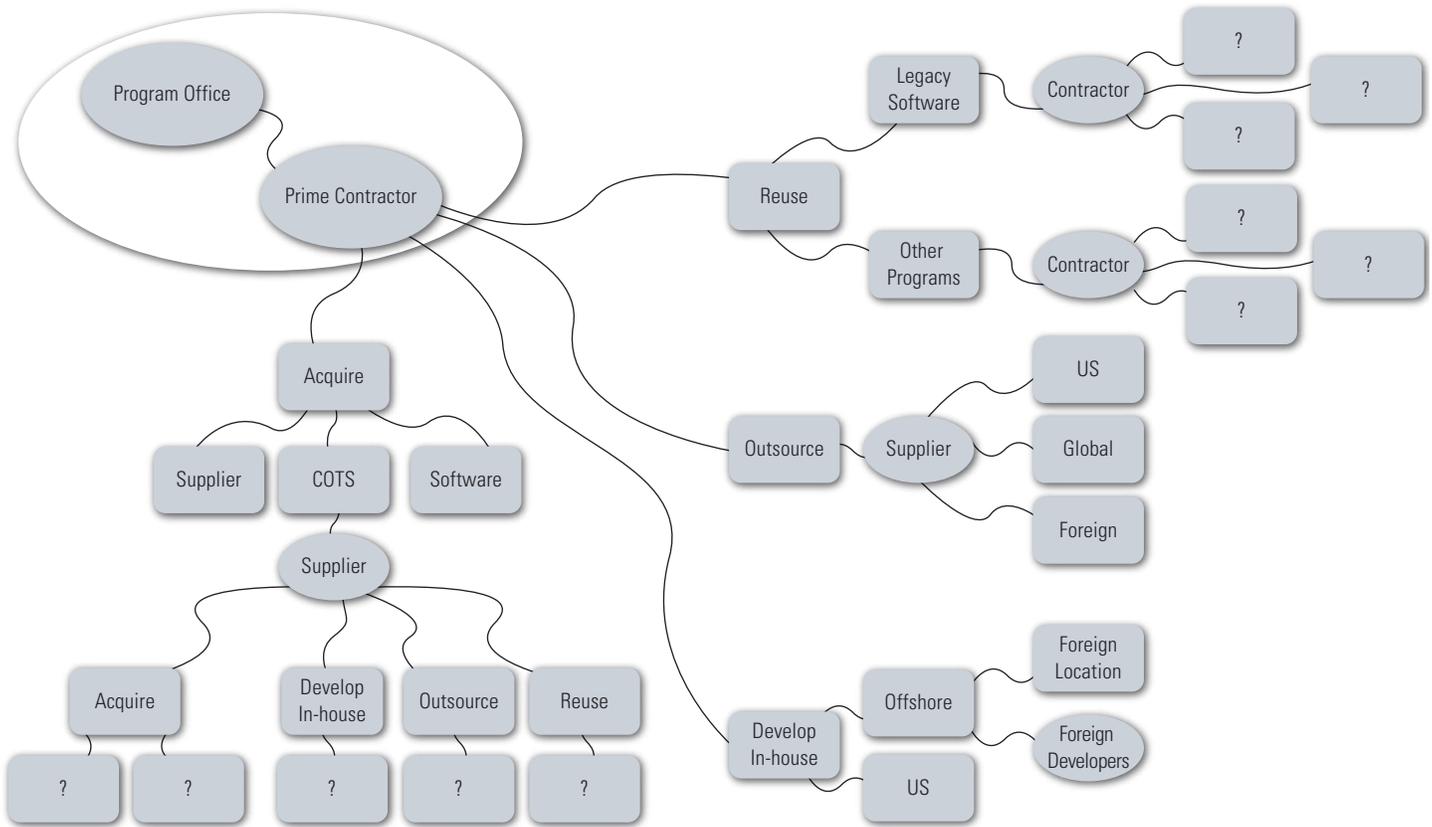


Figure 3 Outsourcing requires sophisticated assurance strategy. [12]

compromised. Establishing this trust among an ever-increasing network of partners and allies poses a great challenge for government agencies and their contractors. In the interconnected and outsourced world, it becomes extremely challenging to provide assurance that the product was developed by trusted developers who used mature processes and procedures. Therefore, having assurance that the system does what it is supposed to do and does not do what it is not supposed to do is virtually impossible.

Industry and government standards, frameworks, and maturity models can help. Buyers can require suppliers to certify how they conduct business and develop their products to provide needed assurance. Although it does not fully protect from malicious acts, it reduces the risk that vulnerabilities were inadvertently introduced due to lax process and procedures. Furthermore, use of standards, frameworks, and maturity models increases probability that vulnerabilities are found *before the product is imple-*

mented, regardless of whether they were introduced accidentally or on purpose.

Measuring, assessing, and reporting interoperability, as a part of an overall assurance strategy, provides direction that is critical for setting the right priorities. Using an interoperable and compatible set of requirements is key to ensuring interoperability. Several existing efforts are facilitating interoperability of requirements, including the DoDAF and DIACAP.

DoD has developed the DoDAF to provide an outline for developing a systems architecture or enterprise architecture (EA). All major DoD weapons and IT system procurements are required for developing and documenting their EA architecture using the set of views detailed in the DoDAF. The benefit of DoDAF is that it provides completeness and consistency across systems—a critical component for interoperability and security. [5] The framework separates statements of operation from descriptions of system mechanism, as well as from the statement of applicable technical stan-

dards, which makes it easier to compare different solutions. The reduced effort spent on translating systems simplifies the task of integrating systems and increases the detection of incompatible approaches while it is least consuming and expensive to resolve them. DoDAF also shifted the DoD's focus from simply collecting documents to a more efficient process of capturing the knowledge and data items pulled from documents and putting them in accessible repositories. This architecture of what an organization knows reduces redundant effort, eliminates opportunities for inconsistency, and guides the way to more streamlined processes. [6]

The DIACAP is the DoD's largest movement for securing Net-Centric operations using repeatable processes to facilitate risk management and apply it to all Information Systems. It provides visibility and control during the implementation of IA capabilities and services, as well as the certification and accreditation (C&A) process for DoD information

systems from core enterprise services (CES) to applications. [7] DIACAP is a great resource because it provides a formal standard set of activities, general tasks, and management structure processes. This allows for the C&A of DoD information systems that will maintain the IA approach throughout the system's life cycle. Those seeking more information can locate it at the DIACAP knowledge base hosted online for users who meet the requirements at <https://diacap.iportal.navy.mil>. The site hosts a DIACAP Instruction guide, DIACAP training and information about recent DIACAP developments, and DIACAP community forums.

Getting the Right Balance

It is understandable that most organizations are seeking a balance between having a reliable, secure, and interoperable infrastructure without spending a fortune on IA, tying up resources, or subjecting their information assets to unacceptable risk. Standardizing business processes helps manage the risks of outsourcing and, if implemented well, can ensure availability of assurance evidence that the requirements have been implemented as stated. Implementing a standard enterprise-level process to replace many similar processes can yield productivity improvements and cost savings.

In a recent article in *IT Business Edge*, the DoD was featured because it effectively implemented a standard procurement system (SPS). The SPS is an

automated contracting system that standardized procurement processes across DoD, replacing more than 70 separate purchasing and contract management applications used within the department. SPS facilitates ordering and delivery materials, supplies, and services for America's warfighters. DoD created a web-based version of its procurement system that has more than 43,000 users in 800 locations. In a DoD statement, the effort had made operations 70 percent more efficient and saved more than \$1 billion simply by reducing accounting errors, system failures, and processing time. [8]

Just like "putting the cart before the horse," the same principle of delivering a product and then testing it makes little sense. Consequently, incorporating standards and best practices should not come after delivery; rather, it should become a part of the initial program or system development. Creating and using improvement processes and procedures saves time and money as opposed to patching systems or working around issues. Northrop Grumman achieved a 13:1 return on investment (ROI), calculated as defects avoided per hour spent in training and defect prevention because they were able to move to CMMI maturity level 5. [9]

Having standards and processes in place avoids many challenges associated with modifying applications or systems at the end of a cycle. Avoidable challenges include systems or applications that can become too slow at transmitting informa-

tion, or may simply fail to deliver information because of inefficient coding. The potential for security violations increases because the software now suffers from an inability to run specific programs at specified times resulting from a poorly functioning system caused by inefficient testing and integration during later stages of development. Similarly, having appropriate processes in place simplifies creating new agreements with vendors all over the globe and provides consensus that they will be followed. Procedures can be improved or modified over time as needed to accommodate new demands and requirements.

Companies are getting greater value out of incorporating best practices and repeatable processes into their business and operations models than just meeting requirements or standards—they are getting meaningful results, cost savings, and risk reduction. A Raytheon Corporation site was able to reduce its rework by more than 42 percent over a several year period after it became a CMMI maturity Level 3 organization. Results from Northrop Grumman Information Technology, Defense Enterprise Solutions, achieved similar results. Figure 4 shows changes over a 3.5-year period. In the first build, the project underestimated its costs; however, by build 6, the organization was able to complete the work for less than initially estimated. [10]

Summary

Today's world calls for organizations to deal with complex connectivity, increased immediate security risks, and interoperability requirements. Organizations are responsible for meeting warfighters' unique demands, sharing knowledge reliably and securely, and responding to threats efficiently. Organizations must strengthen their own infrastructure to be effective, reliable GIG members. Incorporating standardized processes and procedures allows government and industry organizations to leverage their resources and respond to challenges and threats with reliable speed and accuracy. Standard processes and architecture allow interoperability and provide improved security and response

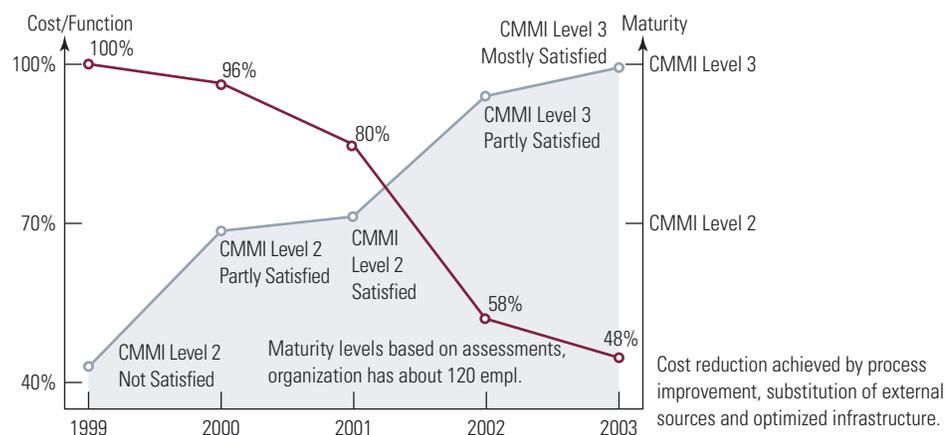


Figure 4 Result of Incorporating Best Practices

because teams know what threats exist and how to react to any situation. Measures can be used to evaluate systems and teams and allow managers to make adjustments to facilitate improvement when needed. Repeatable processes and procedures will streamline operations by eliminating redundant actions and rework.

Numerous industry and government standards, frameworks, and maturity models provide guidance on improving processes to achieve cost and productivity improvements and to increase assurance that the IT infrastructure will provide appropriate support to the mission. Implementing them requires long-term management commitment, stakeholder involvement, and dedication from the organizations that embark on improvement efforts. These efforts aim at changing the fabric of the organization—and they therefore constitute a major change. Successful implementation will enable the organizations to handle the increasing complexity of the world around them, respond to new demands, and create better solutions for the challenges of tomorrow. ■

References

1. GlobalSecurity.org, Global Information Grid (GIG). Retrieved from: <http://www.globalsecurity.org/intell/systems/gig.htm>
2. Managing Technology: The weakest link: Keeping your data secure in a collaborative business environment. Knowledge @ W.P Carey, Published: October 25, 2006 Retrieved from: <http://knowledge.wpcarey.asu.edu/index.cfm?fa=viewArticle&id=1320>
3. Secure Systems Engineering- Capability Maturity Model. Retrieved from: <http://www.sse-cmm.org/index.html>
4. CMMI Performance Results, SEI online. Retrieved from: http://www.sei.cmu.edu/cmmi/results/state_27.html
5. DOD Architecture Framework v 1.0. February 9, 2004. Retrieved from: http://www.dod.mil/cio-nii/docs/DoDAF_v1_Volume_1.pdf
6. Coffee, Peter. Mastering DODAF Will Reap Dividends, eWeek.com. Retrieved from: <http://www.eweek.com/article2/0,1895,1747325,00.asp>
7. Interim Department of Defense Certification and Accreditation Process Guidance. July 6, 2006. Retrieved from: <http://iase.disa.mil/ditscap/interim-ca-guidance.pdf>
8. Flynn, Erin. Military Information Technology Online Archives: Procurement Standard. August 14, 2006, V.10, I. 7. Retrieved from: <http://www.itbusinessedge.com/item/?ci=19593>
9. Secure Systems Engineering- Capability Maturity Model. Retrieved from http://www.sei.cmu.edu/cmmi/results/state_6.html
10. Gibson, D., Goldstein, D., Host, K. Performance Results of CMMI- Based Process Improvement, Software Engineering Institute. August 2006. Retrieved from: http://www.sei.cmu.edu/pub/documents/06_reports/pdf/06tr004.pdf
11. National Strategy for Homeland Security. Office of Homeland Security. July, 2002. Retrieved from: http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf
12. "Scope of Supplier Expansion and Foreign Involvement" graphic in DACS www.softwaretech-news.com Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks."

About the Authors

Nadya Bartol, CISSP, | has more than 13 years of information technology (IT) and information assurance (IA) experience, including IT security and IA performance measurement; security policy development; security architecture design; IT security requirements analysis and traceability; IT security configuration documentation development; risk assessments; certification and accreditation (C&A); project management; process analysis; strategic planning; database management; configuration control; and system analysis, design, development, implementation and maintenance .

In the past 10 years, Ms. Bartol has focused on developing and implementing information security performance management service offering and has established herself as an internationally known authority on information security performance management. She as co-authored National Institute of Standards and Technology (NIST) Special Publication (SP) 800-80, Information Security Performance Measures Guidance; NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Process; and NIST SP 800-55, Security Metrics Guide for Information Technology Systems. She led and advised multiple information security performance management engagements with government and commercial clients.

Ms. Bartol serves as United States delegate to the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) JTC1 SC27 where she is US technical expert working on the ISO/IEC 27000 series standards, Information Security Management System, and a US Head of Delegation (HOD) for Working Group 1. She also chairs the International System Security Engineering Association (ISSEA) metrics working group and is an ISSEA board member. Ms. Bartol is a member of the US International Committee for Information Technology Standards (INCITS) Cyber Security 1 (CS1) technical committee.

Eric White | a member of IATAC, provides program management support to the Joint Task Force–Global Network Operation (JTF-GNO) and to the Defense Components, Law Enforcement and Counterintelligence Center (LECIC), co-located at the JTF-GNO. He has extensive experience supporting operational information assurance (IA) and computer network defense (CND) analysis. Mr. White holds a BA in Criminology from Saint Leo University and an MS in Information Systems and Telecommunications from the Johns Hopkins University.

Stephanie Shankles | supports process improvement efforts across the civilian and government arena. She has previous experience in government public key infrastructure (PKI) operations environments and the customer support arena. She has assisted in implementing CMMI level 3 on the project level. Her background includes a BS in Aviation Management and Flight from Florida Institute of Technology and an MBA in Information Technology from the University of Phoenix.

Michele Moss, CISSP, | is a security engineer with more than 12 years of experience in process improvement. She has assisted numerous organizations with maturing their information technology, information assurance, project management, and support practices through the use of the capability maturity models including the CMMI, and the SSE-CMM. She specializes in integrating security processes and practices into project lifecycles. Ms. Moss is an active member of the Systems Security Engineering Community. She is a Certified Information System Security Professional (CISSP), is an active member of the International Systems Security Engineering Association (ISSEA) and is the Co-Chair of the DHS Software Assurance Working Group on Processes & Practices and Practices.