Making GIG Information Assurance Better Through Portfolio Management

Thomas E. Anderson
GIG Information Assurance Portfolio Management Office

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

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

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

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

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

What Is PfM?

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

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

What Is the GIG?

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

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

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

				Form Approved OMB No. 0704-0188

Report Documentation Page

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

4. TITLE AND SUBTITLE **Making GIG Information Assurance Better Through Portfolio Management**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **517 SMXS MXDEA,6022 Fir Ave,Hill AFB,UT,84056-5820**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**4**	

Standard Form 298 (Rev. 8-98)
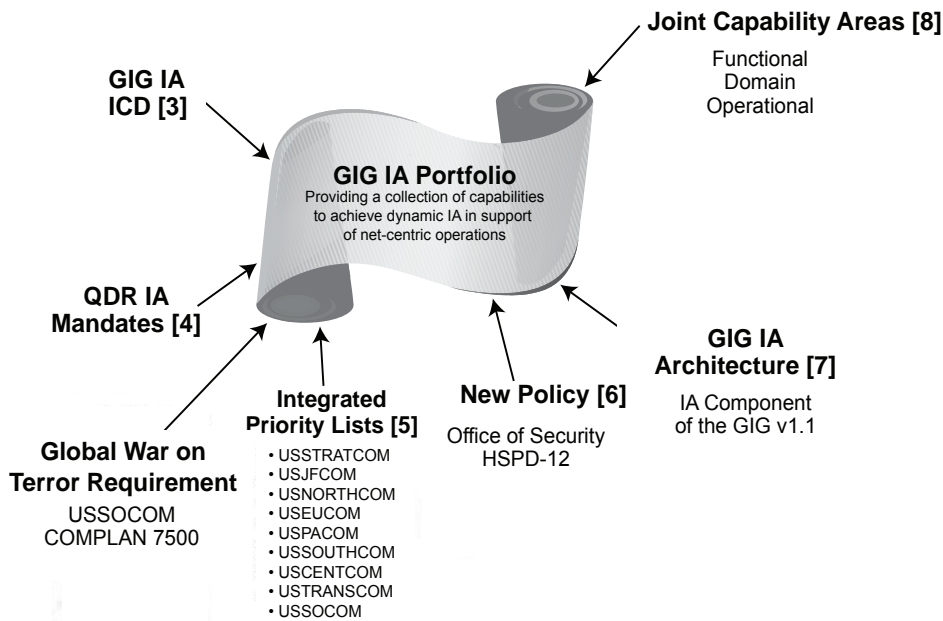Prescribed by ANSI Std Z39-18
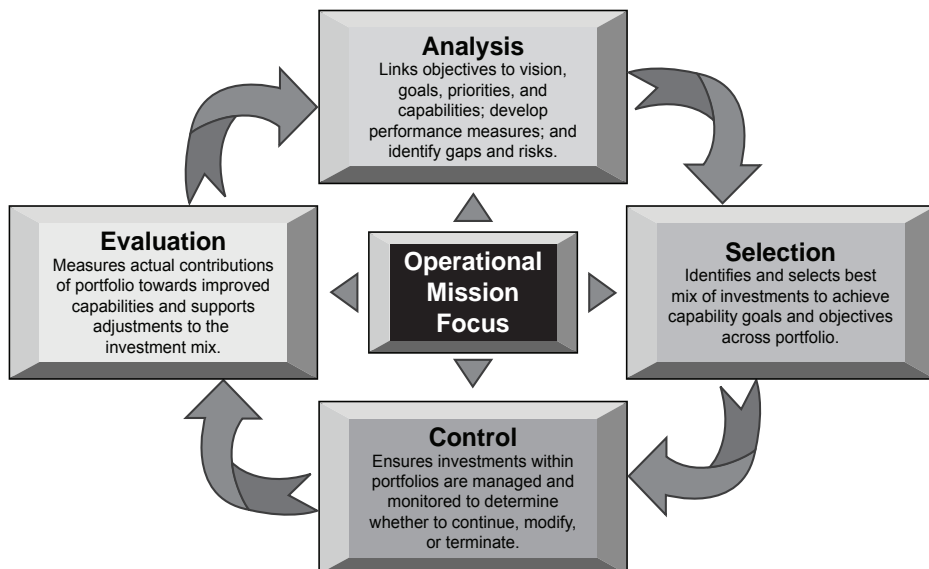
Figure 1: *GIG IA Portfolio Drivers*

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

The GIG will create an environment in which users can access data on demand from any location without having to rely on (and wait for) organizations in charge of data collection to fully process and disseminate the information. With its timelier data availability and more robust communications infrastructure, the DoD expects the GIG to enable more expedient execution of military operations, collaborative mission planning and execution, and common views of the battlespace. The realization of the net-centric vision

depends on sound IA mechanisms being woven into the very fabric of the GIG. Reaching the GIG vision relies to a great extent upon each individual program manager understanding and being willing to be guided by the tenets of the GIG. Applying the tenants of PfM, the strategy for weaving IA into the GIG, consequently, has three main prongs:

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

tional technology upon which the programs will be relying.

What Is GIAP?

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

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

Key IA organizations have been appointed as functional leads to support the IA domain agent in developing and executing a coordinated, DoD-wide IA portfolio. The functional leads are:
- Architecture – NSA IA Directorate.
- Integration – DISA.
- Operations – Commander, U.S. Strategic Command.
- PfM – GIAP Management Office.

So Why Have a GIAP?

As the domain owner, the DASD(IIA) has directed the GIAP Management Office to provide a collection of capabilities that will achieve dynamic IA in support of net-centric operations. The primary focus of the GIAP Management Office is to do the following:
- Recommend the best mix of investments, and synchronize milestones and dependencies to achieve the GIG IA vision.
- Fully leverage baseline resources from research to de-commission.
- Identify approaches to close all capability gaps.
- Monitor execution of investment strategies.
- Measure outcomes and processes and take corrective measures as necessary.

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

Figure 2: *PfM Process*

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

Division of the GIAP Into Capability Areas

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

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

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

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

- Defining architecturally framed technology evolution strategies.
- Providing practical details that describe implementation progress necessary to counter adversaries, close

---

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

---

gaps and vulnerabilities, and achieve net-centricity.
- Identifying programmatic dependencies and synchronization markers.

What Lies Ahead

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

References

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

About the Author

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

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

Acronym Key for This Issue

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