Department of Defense Information Assurance Programs and Cost Control

Doing everything we can to make every defense dollar count

Topic Summary

Information Assurance programs reduce costs and increase quality because:

- Secure and redundant environments reduce risk from both natural and physical threats.
- Well-defined and equitable employment policies and practices motivate the workforce.
- Effective ethical training empowers workers to deliver on requirements.
- Thorough risk management allows the program to complete its mission cost-effectively.

This paper recommends improvements to an operational Information Assurance Program and specifies how these improvements can help to control costs.

Executive Summary

The country's current economic and political climate demands that government contractors rise above "business as usual." President Obama called for tens of billions of dollars in cuts from the Department of Defense (DoD) budget and a five-year domestic spending freeze in his 2011 State of the Union address.[*] Similarly, Defense Secretary Gates called for $100 billion dollars in cost savings over the next five years throughout the DoD in an earlier speech at the Pentagon.[**] Elsewhere in the federal government, U.S. Chief Information Officer (CIO) Kundra's 25-point program to reform information technology management and reduce overall costs emphasizes a "cloud-first" acquisition methodology and requires the termination of "at least one-third of underperforming projects" within the next eighteen months.[***]

DoD spending accounted for 24% of total federal outlays in 2010 and makes an obvious target for lawmakers seeking to reduce expenditures.[****] Managers and executives at every level within both the DoD and private industry must work together to ensure that technology solutions provide demonstrable and value-driven results for the nation. This paper highlights an operational Program of Record (POR) that demonstrates how an effectively implemented Information Assurance (IA) program provides cost control and (to use Secretary Gates' words) does "everything we can to make every defense dollar count."

An IA program provides the confidentiality, integrity, and availability required by DoD information systems. Human beings constitute the weakest link of any organization; the risk posed by even the most dangerous computer hacker is no worse than the damage that could be inflicted by a malicious insider, and errors and omissions still rank highest in overall damage levels.[*****] IA programs must therefore be broad in scope, incorporating both personnel management and operational security (OPSEC). The POR's proactive IA program has targeted several key areas to help it to achieve its mission cost-effectively, including the following:

- It has established strong OPSEC throughout the program.
- It has defined effective employment practices which helped it to create a qualified and motivated workforce.
- It has used Security Awareness Training (SAT) programs to inculcate that workforce with ethical decision-making skills.
- It has implemented a standards-based Risk Management (RM) process that continuously identifies, evaluates, and reduces risks to the POR's organizational goals and objectives.

By adopting this same proactive stance and working hard to wring the maximum value possible from every Defense dollar, other DoD programs and projects can benefit from the RM and IA techniques advocated here to control costs while continuing to deliver on their mission to support the Warfighter.

---

[*] Barack Obama, "Remarks by the President in State of Union Address," January 25, 2011, http://www.whitehouse.gov/the-press-office/2011/01/25/remarks-president-state-union-address (accessed: February 18, 2011).

[**] Robert Gates, "Statement on Department Budget and Efficiencies," January 6, 2011, http://www.defense.gov/speeches/speech.aspx?speechid=1527 (accessed: February 18, 2011).

[***] Vivek Kundra, "25 Point Implementation Plan to Reform Federal Information Technology Management," December 9, 2010, http://www.cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf (accessed: February 18, 2011).

[****] Office of Management and Budget, "Summary Tables," *Budget of the United States Government, Fiscal Year 2011*, http://www.whitehouse.gov/sites/default/files/omb/budget/fy2011/assets/tables.pdf (accessed: February 18, 2011).

[*****] Thomas Peltier identifies accidents, errors, and omissions as accounting for more losses than deliberate acts (STE03, p 541).

Table of Contents

Illustration Index

Tables Index

1.0 Introduction

1.1 Overview

This paper describes how an operational program of record (the POR) within the Defense Logistics Agency (DLA) is controlling costs by using an effective IA program. (For confidentiality reasons, the POR is not identified.) Citizens and lawmakers alike require public funds to be spent wisely and to produce value. The funding of specific programs and projects which do not meet these requirements can and should be cut, especially during this time of increasing federal budget deficits. Adding to this difficulty, and despite the fact that the DoD has scheduled cost-savings plans for the next five years, new initiatives such as CyberCommand[1] require funding support. To succeed in this challenging fiscal environment, each Service within the Armed Forces must scrutinize its spending choices carefully and optimize its existing programs to reduce costs.

IA can help in this mission to reduce costs while actually improving productivity, quality, and capabilities by targeting four key attributes of the DoD's overall security posture:

- *A Hard Shell.* Provide secure and redundant environments for workers and machines.
- *A Motivated Workforce.* Create and implement well-defined and equitable employment practices and policies to attract and retain the qualified talent necessary to accomplish more with less.
- *Ethical Empowerment.* Implement a fully defined ethics program within the IA program, POR employees at every level (contractors, civilians, and active duty personnel) must understand their roles and responsibilities in supporting the larger mission. Additionally, this ethical knowledge enables employees to detect and report deviations from plan before problems escalate.
- *Able Execution.* Develop the IA program according to a Risk Management (RM) methodology grounded in best practices to shield the POR from failure even as it yields superior results.

The ultimate beneficiary of each DoD program is the 22-year-old Soldier in harm's way[2]. The remainder of this paper analyzes how the POR is using its IA program address these key elements and control costs without compromising support for that Soldier.

[1] The U.S. Cyber Command (USCYBERCOM) plans and coordinates the defense of DoD computer networks and, when directed, operates to conduct full-spectrum cyberspace military operations to achieve information dominance over our adversaries. USCYBERCOM achieved Initial Operational Capability (IOC) on May 21, 2010. Source: "U.S. Cyber Command Fact Sheet," *www.defense.gov*, http://tinyurl.com/cybercom-facts (accessed: February 16, 2011).

[2] For 2009, the average enlistment age for the regular Army was 22. Source: "Frequently Asked Questions about Recruiting," *Support Army Recruiting*, http://www.2k.army.mil/faqs.htm#age (accessed: February 6, 2011).

1.2 Definitions

The DoD's authoritative set of definitions for information security terms lays a firm foundation upon which to build an IA program. In fact, the DoD's definitions and standards have often served as the basis for the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-Series of papers; these NIST publications are used throughout the federal government and commercial sectors to implement IA programs.[3]

The DoD defines Information Assurance as consisting of "[m]easures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" (CNSSI 4009). Moving on to the IA components analyzed by this paper, one finds the following definitions:

Operational Security (OPSEC): "A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities" (DODD-5205).

Employment Practices: "Promote stability of employment for civilian employees affected by changing workforce requirements[; …] Maintain a strong placement and transition assistance program to minimize […] adverse effects on employees[; … and,] Ensure employees are treated equitably and uniformly"[4] (DODI-1400).

Ethical Standards: "DoD Agencies shall administer and maintain a comprehensive Agency ethics program[; …] No DoD Agency shall […]restrict or modify this Directive […]without approval[; … and,] DoD personnel shall perform their official duties lawfully and comply with the highest ethical standards. Heads of the DoD Agencies shall ensure that the Agency ethics program is maintained and that sufficient resources are provided […] to execute an effective Agency ethics program"[5] (DODD-5500).

Risk Management: "The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation or use of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and 4) documenting the overall risk management program" (CNSSI-4009).

All four of these components are required for an IA program to be comprehensive.

[3] The reader is invited to visit NIST's Special Publications home page at http://csrc.nist.gov/publications/PubsSPs.html for more information (accessed: February 2, 2011).

[4] Paraphrased from the Instruction.

[5] Paraphrased from the Directive.

2.0 The IA Program and Cost Control

2.1 IA and Overhead

IA is sometimes dismissed as unproductive overhead required for an organization to demonstrate compliance to arbitrary laws and regulations. However, nothing could be further from the truth; as John Caughell pointed out in 2010, "overhead is not a bad thing, it is actually necessary."[6] After all, receptionists, security guards, accounting functions, and every "C"-level officer within a company are, themselves, overhead. Overhead provides the basis for a successful enterprise; without overhead a profit center cannot operate. Considering that the DoD must maintain extensive sets of classified information to accomplish its mission and that the primary goal of IA is to enable an organization's success by protecting information and the systems surrounding information, IA expenditures within the DoD are money well-spent.

IA goes beyond simply protecting information; correctly implemented IA cuts costs. Given the country's current fiscal woes, Congress is particularly eager to see such savings realized. On the other hand, improper implementation of IA offers no such benefit. As an analogy, consider keeping a house as secure as possible: simply sheathing the entire structure in iron certainly appears to solve the problem. In the same way, when presented with information to protect, it is all too easy simply to apply every security control imaginable. Both approaches fail in practice. Iron sheathing would render a house uninhabitable (failing one of the core tenets of IA),[7] and its apparent security would be illusory; the concentrated use of muriatic acid would defeat the iron sheathing quickly.[8] Just so, careless application of Information Security (INFOSEC) controls quickly increases costs without genuinely enhancing security. Worse yet, unnecessary INFOSEC controls actually degrade overall Information Assurance due to unintended and unplanned side effects, such as the inability to access the data necessary to make a business decision in a timely fashion (akin to the inability of a house's inhabitants to access their ironclad home).

The remainder of this section discusses the core IA components defined in Section 1.2 above and shows how each component helps to provide effective IA while controlling (or even reducing) costs:

- *Operational Security (OPSEC)* includes guarding the POR's physical infrastructure and ensuring that security policies are enforced.
- *Employment Practices* affect how the POR hires, retains, and develops the capable people necessary for a smooth operational environment. Key to the POR's success is the training that employees receive on how to make good and ethical business decisions.
- *Risk Management (RM)*, as typified by the POR's RM program, identifies the vulnerabilities within its information systems and reduces risk by applying mitigating controls against the set of credible threats to those vulnerabilities.

---

[6] John Caughell, "Planning for 2011" [Weblog Entry], *Constant Profit Advisors*, July 29, 2010. http://johncaughell.wordpress.com/2010/07/ (accessed: February 10, 2011).

[7] Confidentiality, Availability, Integrity, Control, Usability, and Authenticity make up the generally-accepted set of primary IA tenets. By preventing the owners from entering the home, the iron sheathing has impacted Usability.

[8] Douglas Godfrey, "Iron Oxides and Rust (Hydrated Iron Oxides) in Tribology©," *Journal of the Society of Tribologists and Lubrication Engineers*, February 1999, pg. 35.

2.2 Operational Security (OPSEC)

2.2.1 Overview

A correctly-implemented OPSEC program forms a hard shell around an organization. OPSEC includes both an organization's day-to-day enforcement of its security perimeter (both logical and physical) and its implementation of defense in depth. OPSEC ensures that employees follow defined procedures while performing their assigned tasks and that secure facilities maintain their integrity by controlling ingress and egress. Within Information Technology (IT), OPSEC avoids costs by preventing the losses which would stem from incorrect or unauthorized computer system access or data modification. Within the physical world, OPSEC controls cost by ensuring the integrity and availability of facilities and equipment. As with all aspects of IA, however, poor implementation of OPSEC results in less effective actual security and a lower return on investment (ROI).

2.2.2 OPSEC and Defense in Depth

Correctly implemented security programs function much like the layers of an onion, security controls becoming more refined with each layer. Called "defense in depth," this concept is a cornerstone of IA and emphasizes the importance of including technical, administrative, and physical controls supported by the entire organization. This section identifies two ways in which the POR implements defense in depth.

Figure 1: Defense in Depth[9]

2.2.2.1 Logical Defense in Depth: Workstations

The POR uses OPSEC to implement a number of logical controls on the computer workstations assigned to POR employees:

1. *User login*. Each workstation requires identification (the identity claimed by the user), authentication (verifying the user's claimed identity), and authorization (checking the user's access level for this

[9] Source: National Security Agency, "Defense in Depth," http://www.nsa.gov/ia/_files/support/defenseindepth.pdf (accessed: February 9, 2011).

system). Lower-security workstations, such as those located on unclassified networks, use only a simple user name and password. Higher-security workstations, such as those belonging to a classified network, require strong authentication[10] with a Common Access Card (CAC).[11] Optimally, all computer logins should require strong authentication using the CAC.

2. *Application execution*. End-users are granted access to different software applications based on their assigned roles; a developer requires a programming environment while a manager requires project management tools. A user can run only the software authorized for his or her workstation; furthermore, the capability must exist for authorized software packages to be automatically "pushed" to newly assigned workstations upon first login by any given user. The POR uses Group Policy Objects (GPOs) to automate application deployment but could more easily control a large set of workstations by using a specialized desktop management system. This separation of duties demonstrates how an IA program must be supported by the entire organization: managers and executives to define roles and responsibilities; human resource personnel to support those roles; and IT Operations to implement these roles by controlling each employee's desktop experience. This paper's recommendations identify how the POR can leverage commercial tools to centralize and economize this control.
3. *Data access*. The POR manages numerous data sets, and as a component of DLA this managed data is among the most valuable on earth (including, for example, troop movements and dispositions). Data must be available to those entities ("Subjects") that "dominate" the data (possess both the security level to access the data as well as the need to know about the data).[23] By implementing least-privilege data access via both mandatory access controls (MAC)[12] and discretionary use of access control lists (ACLs), the POR ensures that users can see and process only the data to which they possess both clearance and need-to-know.
4. *Remote system access*. All Subjects requiring access to any protected remote system (such as system administrators accessing a production environment, or other DoD data consumers connecting to the POR's infrastructure) must be authorized using Department of Defense (DD) Form 2875.[13] This ensures that traffic to these systems is tightly controlled and that connectivity troubleshooting (as well as activity auditing) can be performed.

These controls work together to refine protection as users advance within an information system and are just a few of the functions that an OPSEC program must provide.

[10] Authentication using any two of something the user has (a physical object), is (Biometrics), or knows (passwords and so on).

[11] The DoD provides a Common Access Card, or *CAC*, that contains an encrypted and highly-protected private key for each active-duty or retired military person and his or her dependents (see http://www.cac.mil/ for information). DoD also provides CACs to civilian workers and DoD contractors (contractors require sponsorship).

[12] Mandatory access controls are those data access rules which *must* be followed, while discretionary access controls (DAC) are data access rules that can be assigned by the data owner. For example, top-secret data can never be released to someone who has only a secret clearance; this is an example of MAC. (To be precise, MAC requires both clearance and need-to-know.) On the other hand, unclassified data within a given department can have read / write permissions granted to individual users by the department manager; this is an example of DAC. Other types of access controls also exist; see the reference for more information (BOS09, p 282-285).

[13] DD Form 2875 ("System Authorization Access Request") requires identification of any entity accessing a protected military system, including the reasons for access and the authorizing authority.

2.2.2.2 Physical Defense in Depth: Redundancy

For the POR to accomplish its mission, the data centers it manages must be highly available. In the event of a failure within one center, another must instantly respond to the outage. To ensure Continuity of Operations (COOP), redundancy of data centers requires communications between the sites to be maintained, required data sets to be replicated from the production site to the backup site, and controlled outage tests to be periodically conducted to verify that Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) can be met.[14] The POR's OPSEC team follows policies and procedures to maintain communication lines and to perform regularly scheduled tests of catastrophic recovery measures (such as the failure of an entire data center).

2.2.3 OPSEC and Cost Control

The POR's goal of high availability puts the amount of tolerable system downtime at 8.76 hours per year, or "three nines."[15] According to the Project Management Institute (PMI), the "number of nines" of reliability for a project's deliverables relates directly to its quality-management planning, and such planning always results in lower operational costs (PMI, p 221-222). The POR's ongoing OPSEC processes support this quality planning by enabling frequent communication with stakeholders and end-users to ensure quality (defined as "conformance to requirements," such as meeting Service Level Agreements. Additionally, OPSEC processes enforce a sound configuration management process that analyzes changes to prevent defects from tainting production systems and holds management accountable for meeting system uptime requirements.

The POR's current OPSEC practices and approaches result in the effective delivery of data to authorized consumers and support the DLA's organizational mission. By minimizing the risk of outages and ensuring that data is highly available to meet Service Level Agreements (SLAs) with its customers, the POR's OPSEC yields demonstrable cost benefits.

2.3 Employment Practices

2.3.1 Overview

The POR provides data integration and access services to the DLA and consists of groups of highly technical individuals from disparate DoD prime contractors and subcontractors. These skilled and specialized employees must be able to work within the POR's secure environment. Thus, the POR has defined and implemented a comprehensive set of employment practices that allow workers to be onboarded, made operational, and

[14] RTO is the maximum service interruption permissible for resumption of normal service, while RPO is the maximum permissible data loss acceptable during any outage (BOS09, Chapter 62). Losses beyond this time period indicate a severe problem that could affect the POR's ability to achieve its mission.

[15] Uptime to three standard deviations from the mean ("three sigmas") translates to a defect (downtime) rate of ~ 0.01% or 8.76 hours per year (~ 99.9% uptime, or "three nines") (ALLEN10, p 19). The reader is also perhaps familiar with the term "Six Sigma," which corresponds to ~ 99.999999% reliability ("eight nines") and is also the name of a business management strategy created by Motorola in 1986 which emphasizes quality planning and control to achieve a 99.99% success rate in their manufacturing process. Motorola's Six Sigma program has been adapted to a variety of industries and disciplines.

terminated; all in an efficient and cost-conscious manner.

2.3.2 Onboarding

The DoD is subject to the same hiring constraints as other federal agencies, with some important exceptions. For example, the Immigration and Reform Act of 1986 specifies that employers cannot impose citizenship requirements on its workforce but provides exceptions "required in order to comply with law, regulation, or executive order" for areas such as national security (PL08). Within the POR, the employment process requires an extra set of steps to ensure that program objectives are met; these steps are described below.

2.3.2.1 Planning for Onboarding

The POR's onboarding management processes began life prior even to the official start of the program. As with all significant DoD contracts, the Request for Quotation (RFQ) sent to prospective prime contractors defined the POR's overall employment requirements. Each submitted quotation had to include a "Management Approach" section that laid out how the contractor intended to satisfy these requirements. A full listing of program requirements cannot be detailed here, but some of the high-level items included:

1. *Allowed Job Classifications*. The contractor had to staff the POR using only job classifications identified within the RFQ (such as Systems Architect or Database Administrator). These job classifications have specific meanings and requirements based on the contract terms. After contract initiation these job classifications can be changed only via Standard Form (SF) 1444 ("Request for Authorization of Additional Classification and Rate") in conjunction with written agreement from the government-assigned Contract Officer (KO).
2. *Security Processing.* The contractor had to identify how it intended to integrate with DoD security clearance requirements; for example, how it intended to gather and submit SF 86 ("Questionnaire for National Security Positions"). Additionally, the contractor retains responsibility for holding ("billeting") all granted security clearances for employees brought on to the POR throughout the life of the contract.
3. *Service Contract Act of 1965 (SCA)*. The contractor had to demonstrate how it would meet SCA requirements for providing minimum safe workplace conditions and fair payment scales for all employees, excepting those persons who met "bona fide executive, administrative, or professional" status (PL41).
4. *Information Assurance*. The POR's implementing prime contractor had to list explicitly how it intended to satisfy IA requirements based on the following sets of guidance:
   a. DoD and Chairman, Joint Chiefs of Staff (CJCS) requirements and
   b. Joint Task Force – Global Network Operations (JTF-GNO) taskings.

   The full solution was presented to the government as a completed Information Assurance and Industrial Security Plan (IA&ISP).

Finally, each quotation had to include an overall Integrated Program Management Plan (IPMP) that identified and planned for all program requirements throughout the POR's lifecycle.

2.3.2.2 The Onboarding Process

The POR delivers complex information systems to the DLA; thus, many onboarded employees are highly

technical individuals. The POR follows many of the best practices laid out by Dr. Ronald Kandt of the Jet Propulsion Laboratory for bringing on software engineers (STE03, p 253-271):

1. *Conformance to Job Requirements*. All job candidates must be interviewed at least twice, and at least one interview must include a technical representative skilled in the technology(s) listed in the job classification. Per Dr. Kandt's suggestions, candidates must demonstrate domain knowledge beyond their specialization. Candidates possessing such knowledge are well-suited to cross-training in support of initiatives being undertaken throughout the POR. As an example, Java programmers must demonstrate proficiency in at least one other technical domain (such as Oracle database administration or C# programming).
2. *Verified personal background.* All candidates must possess at least a secret clearance. Field Security Officers (FSOs) administer SF 85 ("Electronic Personnel Security Questionnaire"), collect candidate fingerprints, and perform citizenship verification. This information is stored in a secure and searchable database.
3. *Verified job and educational history*. The personnel office researches the candidate's educational and career claims (including contacting provided references). Beyond that, DODD-8570 ("Information Assurance Workforce Improvement Program") requirements must be met. Employees must be matched to their expected operating classification on computer networks, and possession of any required commercial certifications must be verified for those employees (or obtained shortly after these employees have come on board).[16]
4. *Security Awareness Training (SAT)*. DODD-8570 requires that all onboarded employees take a formal set of training courses and sign a "Statement of Acceptance of Responsibilities." The POR uses training material from the DoD's own Information Assurance Support Environment (IASE, http://iase.disa.mil/) as well as custom-developed packages.[17]
5. *Employment Agreements*. Each vendor bringing staff onto the POR must ensure that all employees agree to abide by program-wide Acceptable Use Policies (AUPs). These AUPs cover intellectual property (IP) considerations as well as appropriate usage of corporate resources, particularly the proper care and handling of program data.

One potential problem with the above is that each contractor's specific employment policies may differ. The POR's Program Management Office (PMO) does not require these policies to be centrally managed (although all individual company policies must conform to overall DoD requirements). Consolidation of all vendor policies into a single knowledge base averts the possibility for confusion among these individual policy sets.

[16] DoDD 8570.01-M breaks the workforce into both Technical and Management categories, where each category can be one of three classifications (I to III, with III being the highest). Each category / classification has an associated set of training and certifications required for it. As an example, Management Level II must have five years of management experience and appropriate certifications.

[17] The IASE operates under the authority of the Defense Information Systems Agency (DISA) and provides guidance / training programs to Agencies and Services throughout the DoD.

2.3.3 Daily Operations and OPSEC

Section 2.2.2 addressed overall OPSEC within the POR; this section addresses how OPSEC (and the policies which drive it) affects day-to-day operations. The POR depends upon a trained and informed workplace in order to carry out ongoing activities. Because the POR handles both "low-side" (unclassified) and "high-side" (classified) data, special attention must be paid to confidentiality and integrity requirements.

2.3.3.1 Overview

The POR satisfies OPSEC requirements by following DoD Manual 5502.02-M ("DoD Operations Security (OPSEC) Program Manual"); while a complete listing is beyond the scope this paper, some highlights follow:

1. *Program Management.* As described above, the POR has a full IA&ISP that includes documented communication of policies and standards to personnel. The POR performs this communication at onboarding (initial training), at scheduled intervals (no more than one year apart), and on an as-needed basis. As a case in point, consider the premature announcement on February 18, 2010 that the DoD had lifted its 2008 ban on Universal Serial Bus (USB) memory "sticks."[18] This supposed lifting was never true for all of DoD but continued to dog the Department throughout 2010.[19] The POR had to send out at least one mass emailing to clarify the DoD's official policy.
2. *Ongoing Training*. Many individuals are required to hold specialized credentials for their job classifications, such as specific certifications in various Commercial Off The Shelf (COTS) software applications used within the POR. Such individuals must register their credentials with the Program Management Office (PMO) and they must maintain these credentials to continue working in the POR. Additionally, the POR strongly encourages all technical personnel to attend relevant events of interest. As an example, the Information Assurance and Technology Analysis Center provides a clearinghouse of DoD- and IA-related events both online and around the country.[20] Other venues include meetings hosted by such organizations as the Information Systems Security Association (ISSA)[21] and the Project Management Institute (PMI).[22] The expectation is that personnel will maintain and enhance their expertise in their operational areas.
3. *Maintain data classifications and access*. Crucial to safe data exchange within the POR environment is the proper classification of data. The POR uses a Clark-Wilson "access triple" model (CLARKW-87) to control data exchange between the low- and high-sides. This model requires that access to "constrained data items" (classified information) be mediated via "transformation procedures" which apply authorization and access rules by which a requestor (Subject) must have both clearance and need-to-

[18] Kevin McCaney, "DOD lifts ban on USB drives," *Government Computer News*, February 18, 2010. Available at http://tinyurl.com/dod-lifts-usb (accessed: February 7, 2011).

[19] U.S. Strategic Command Public Affairs, "Federal Times clarification - USB policy," *United States Strategic Command Web site*, June 30, 2010. Available at http://tinyurl.com/usb-still-banned (accessed: February 7, 2011).

[20] See http://iac.dtic.mil/iatac/IOcalendar/scheduler_current.html for information on current security events.

[21] ISSA is a leading organization within the IA community and strongly encourages practitioner excellence. See https://www.issa.org/ for more information.

[22] PMI is the premier worldwide organization providing standards and practices for managing projects. See http://www.pmi.org/ for more information.

know to obtain that access.[23] "Unconstrained data items" (unclassified information) are not subject to the same degree of access control. To maintain this level of data classification and access, POR personnel must be knowledgeable of policies governing the data and must be capable of enforcing these policies. Furthermore, the policies cannot be arbitrary; rather, they must be undergirded by relevant laws and regulations.

From an operational view, one area for improvement is to build a cross-linked information system that relates key POR publications (such as Security Guidelines or Acceptable Use Policies) to the authoritative guidance backing them (such as DODD-8570 for certification guidelines affecting POR team members). Currently, changes to authoritative policy drivers like DODD-8570 that affect POR-specific documents must be reviewed and updated manually. Automation of this process would allow the POR to become more agile in understanding and responding to changes within DoD or federal policies.

2.3.3.2 Awareness Training and Ethical Decision-Making

Section 2.3.2.2 listed SAT as an integral part of the onboarding process, and the POR includes ethical training as guided by DLA. All POR team members (both government and contractor) must take SAT at least once per year. Ethical decision-making permeates all aspects of the POR's daily operations, from how workers manage Personally Identifiable Information (PII) to how workers are expected to report their personal time usage.

The POR draws on several resources for ethical decision-making in addition to the IASE resource specified in Section 2.3.3.2. The DLA provides online access to Ethics Training (updated each year)[24] which proffers: guidance on allowed gift exchanges between employees and outside sources, techniques for avoiding even the appearance of conflicts of interest, guidance on the proper use of government resources, and the Code of Ethics for government service. Most importantly, guidance at the DLA level aligns directly to guidance from DODD-5500.7r ("Joint Ethics Regulation"), the "single source of guidance" for all standards of ethical conduct.

2.3.4 Post-Employment

As a Level III program[25] the POR imposes particular requirements upon resources leaving the program (both human and machine, although this paper covers only the human aspect). The POR has based its own IA&ISP on DoD's operating manual 5220.22-M ("National Industrial Security Program"), which is a guidebook for implementers to follow. Employee terminations must conform to relevant sections within the guide (italicized references are to sections within 5220.22-M):

1. *Reporting (1-302.a and 1-302.c)*. As an important program within DoD, the POR must report changes in cleared status (to include any "adverse information") regarding any employee to the "Cognizant Security Agency" (CSA). Thus, the POR mandates that the CSA be notified about any wrongdoing which has been detected. The CSA's representative for the POR is a DLA-assigned Security Officer (SO). This change reporting (especially that of adverse information) is an automated process.

[23] When a Subject has both the clearance necessary to access an Object as well as a verified need to know about that Object, the Subject is said to Dominate that Object.

[24] See http://www.dscc.dla.mil/offices/legal/ethicsinfo/ for all DLA Ethics Resources (accessed: February 1, 2011).

[25] Level III DoD programs consist of "a full-time managed and resourced OPSEC program" that, due to its sensitivity, "requires substantial *[IA]* effort" necessitating a sustainment budget (DODM-5205).

2. *Debriefing (3-108)*. The termination process must include a documented set of conversations during which the employee is made aware of his responsibilities and all POR property is recovered (badges, issued equipment, and so on).
3. *Sanitization (5-309 and 5-313.d)*. Post-employment, all of the terminated employee's accounts must be deactivated; locks for which keys have been issued to the employee must be changed; and, the employee's access to secured areas must be disabled (in case the ex-employee manages to retain an entry card). The POR accomplishes these functions by associating each employee with the set of allowed system and facility access privileges granted to that employee. (The usage of Form 2875 provides the necessary common frame of reference). This allows a standard termination workflow to be invoked and ensures that the employee's access to each affected system is revoked.

One area for improvement is in the overall integration between Operations and Human Resources (HR); specifically, Operations and HR should collaborate throughout the termination process to ascertain that all possible usages of the soon-to-be ex-employee's account(s), within all network environments, have been identified. Special care must be taken to locate systems where the employee's user account has been used to run automated scheduled tasks. Rare though this situation may be, it is a challenge for IT to identify and correct such a circumstance when it does occur.

2.3.5 Employment Practices and Cost Control

Other than the contract requirements highlighted in Section 2.3.2.1 above, the DoD does not actively enforce personnel and employment policies on its contractors.[26] Instead, contractors must execute an awarded contract satisfactorily while simultaneously abiding by all employment laws and regulations issued by the federal government. For example, charges of racial discrimination within a DoD contractor's organization would be reported to the Equal Employment Opportunity Commission (EEOC) rather than to the DoD, although the DoD may terminate contracts where such violations to occur.

Employment practices can reduce costs by improving employee retention and avoiding the expense of non-compliance. Employee retention is critical for any organization; as Daniel Jacobs reported in 2000, "it costs…three to 10 times more to acquire a new employee…than to retain an old one."[27] By creating and applying fair and equitable employment practices that demonstrate the company's commitment to its employees, a company will foment workforce stability. The cost of non-compliance, on the other hand, ensues when employment policies have not been carefully aligned to appropriate laws and regulations. As noted by the National Employment Law Council in April of 2010, the Department of Labor (DoL) concluded almost thirty thousand compliance actions in 2008 based solely on employee complaints relating to wage and time issues, finding violations in eighty percent of those actions and imposing fines totaling almost ten million dollars.[28] The

[26] DODD 1440.1 ("The DoD Civilian Equal Employment Opportunity (EEO) Program") establishes a number of requirements that Heads of DoD Components shall satisfy including training, developing affirmative action programs, procedures for investigating and resolving complaints, upward mobility programs, and much more. However, enforcement of EEO remains under the purview of the EEOC.

[27] Daniel G. Jacobs, "The Cost of Recruiting," *Smart Business Cleveland*, October, 2000 (paraphrased). Available at http://tinyurl.com/cost-of-recruiting (accessed: February 10, 2011).

[28] Lindbergh Porter, "Wage and Hour Updates and Guidance on Audits and Compliance," *National Employment Law Council*, April 30, 2010. Available at http://tinyurl.com/dol-compliance (accessed: February 11, 2011).

report suggests that employers foster a "culture of compliance" and advises that proactive, self-funded audits can avoid complaints and "make good business sense."

Finally, successful employment policies and practices aid a company in a less quantifiable way: company assets are better protected because employees are aware of their stewardship responsibilities. For example, employment policies that clearly identify how an employee should act with regard to data or equipment owned by the company can work in tandem with SAT to prevent the unauthorized dissemination of the asset. In the POR's case, these policies help employees to understand that company data cannot be copied onto removable storage media like CDs or USBs for any reason. To sum up, in order for a company's employment policies and practices to be fully effective, they must be the result of an integrated effort across department lines.

2.4 Risk Management

2.4.1 Effective Execution and Risk Management

RM is the DoD's primary tool for ensuring that a program delivers verifiable and reliable results (DOD-RMG, p 2). RM lies at the heart of every successful DoD project and must be embedded within the project's management and execution methodology. This section examines some of the high-level RM drivers that the DoD and DLA provide as guidance to the POR and at how the POR uses RM to control costs and to improve its overall program quality.

DoD's Risk Management Guide for Acquisitions (DOD-RMG) defines a subset of commonly accepted risk mitigation techniques (p 23):[29]

- Avoid risk by eliminating root causes,
- Control the cause or consequences [of the risk occurrence],
- Transfer the risk, and/or
- Accept ("assume") the level of risk and continue on the current program plan.

Risk should be avoided altogether if such avoidance does not compromise a deliverable's conformance to requirements. Consider the bulk purchase of laptop computers: if a given vendor's product offering does not have a reliable track record, then the risk of defective laptops should be avoided through the use of an alternative source. However, certain risks are inevitable and should, if possible, be transferred to an insurer (homeowner's insurance being a classic example of this approach).

"Controlling the cause or consequences of a risk occurrence" is also referred to as "risk mitigation." One controls the *causes* of a risk occurrence by using preventive techniques; as an example, an organization often deploys a firewall to prevent malicious network traffic from entering or exiting the corporate IT infrastructure. One controls the *consequences* of a risk occurrence by using detective, corrective, and recovery controls. Consider the firewall example just cited: what would happen if an identified risk did occur (such as an inbound computer virus)? The organization would use COTS anti-virus software to detect and report this occurrence and

[29] The standard set of risk mitigation techniques also includes *sharing* and *acquiring* risk. "Sharing" refers to dividing risk between two partners, while "acquiring" refers to the organization recognizing that it has a core competency in managing a specific type of risk (such as network intrusions) and making a business decision to seek opportunities to assume that risk on behalf of customers (STE03, p 308).

would have already defined an incident response plan by which to minimize consequences. Incident response plans allow for even catastrophic failure by implementing recovery controls so that in the aftermath of a catastrophe an organization can return to normal operations as soon as possible.

The key to effective RM is the planning phase. Risk is calculated by considering a vulnerability (such as ineffective window locks on a building, or an insecurely-protected computer on a network) in conjunction with a threat agent (such as a burglar, or a malicious computer hacker). The risk is the probability that a given action will occur (such as the burglar breaking into the building, or a computer being infected with a virus), along with the expense of that occurrence (the "impact").

2.4.2 Risk Management Guidance for the POR

The POR operates within the context of DLA, which itself operates as an Agency within the DoD. Thus, the POR receives at least two layers of authoritative RM policy guidance that it must follow.[30] This section looks at selected key policy drivers from both the DoD and the DLA.

2.4.2.1 DoD Guidance

Numerous DoD Instructions and Directives pertain to RM, three of which appear to address the POR specifically:

- *Ensure Environment, Safety, and Occupational Health (ESOH).* Human and environmental safety is a top priority within any project. The DoD directs that each Program Manager (PM) shall integrate ESOH risk management into the overall Systems Engineering (SE) process for all developmental and sustaining engineering activities (DoDI-5000.02, p 78).
- *Ensure program cost, schedule, and performance objectives are met.* These goals are particularly germane to this paper's focus on using RM to control program costs while preserving quality. To demonstrate compliance to these requirements, each program must define an RM plan that includes the following: a Risk Management Board (RMB), the RM approach being used, the specific RM roles filled by government and industry stakeholders, and how identified risks will be mitigated (DOD-RMG, p 2 - 6).
- *Ensure that projects can be moved successfully from Development to Production.* As a large-scale technology acquisition program with a sizable system development component, the POR must ensure that its employees' hard work results in a reliably deployed system. To accomplish this, the POR must minimize its risks by implementing and following a sound SE methodology (DAG 2010, p 123). A 1985 document sums up this requirement well: "The key word is discipline! [It] help[s] us collectively [to] make wiser decisions on ongoing programs [and] to see whether our decisions and the actions on which they are based fall within the boundaries of an effective and efficient, low risk program" (DODM-4245.7, p 3).

[30] Source: Personal interview, Security Officer within POR, February 1, 2011.

As a part of the DoD's overall program infrastructure, the POR must ensure that its RM plan meets these requirements. The DoD does not define a standardized formal Risk Management Plan; it is up to individual PMOs within each program to ensure that they meet the specified high-level guidelines and policies (DOD-RMG, p 2). To aid PMOs, the DoD provides a sample RM plan that can be used as a template.[31]

2.4.2.2 DLA Guidance

DLA inherits the above guiding principles while focusing on acquisition and operational RM goals. As such, DLA's Risk Assessment and Process Improvement Division (J53) furnishes leadership, policy, guidance, and oversight of Enterprise Risk Management (ERM) within the DLA.[32] The ERM provides the framework that J53 suggests all programs should use (including the POR). The high-level ERM framework is shown below:

Figure 2: J53 ERM Framework[33]

ERM's architectural approach targets the DLA's many layers: Enterprise, Business Units such as the POR, Divisions, and Staff. Individual PMOs must employ a risk-focused management approach that emphasizes root cause analysis in direct support of explicit DoD higher-level guidance (DoDAG, Section 4.2.3.1.5) and are cautioned not to confuse "issues" (realized risks) with true risks (future uncertainties).

[31] See DoD's "Generic Risk Management Plan" (2001) at https://acc.dau.mil/CommunityBrowser.aspx?id=19076.

[32] See http://www.dla.mil/J-5/RiskAssessment.asp for more information on the J53.

[33] Source: J53 ERM cube, http://www.dla.mil/J-5/ERM.asp (accessed February 24, 2011).

2.4.3 Risk Management Use Case

The POR implements RM at the PMO level, the SE level, and the Sustainment level.

2.4.3.1 PMO Level

Throughout the DLA, individual PMOs direct and track specific Risk Management Plans. The POR's PMO tracks its overall project status using Microsoft Project, ties identified risks back to program requirements using International Business Machines (IBM) Rational RequisitePro, and automates and tracks configuration management using IBM Rational ClearCase and ClearQuest. Configuration management is essential to the mitigation of risk and ensures that system changes are carefully analyzed for their potential impacts to the program. As program deliverables are built and deployed, each contractor and government/DoD entity working within the POR can use these tools to manage change; additionally, the POR's PMO provides an online project status/risk reporting mechanism. This mechanism delivers high-level reports to the POR management team; these reports consist of the information the team needs to keep the program on schedule and to identify quality variances sooner rather than later (leading in turn to less-costly defect remediation).

The PMO also ensures that the POR as a whole meets ESOH requirements for RM by:

- Identifying ESOH responsibilities within the POR.
- Integrating ESOH considerations into the Systems Engineering Lifecycle (SELC).
- Requiring each facility used or operated within the POR to comply with environmental and safety standards.

By standardizing on the supporting software tools and holding all POR team members to a common safety standard, the POR's PMO reduces overall program cost and strives to avoid harming individuals or the environment. The POR's PMO publishes high-level project status dashboards and reports for DLA and Congressional oversight committees through its online portal. In so doing, the PMO keeps the POR's stakeholders adequately informed of variances from the POR's schedule, cost, or quality baselines.

2.4.3.2 Systems Engineering Level

SE and RM mesh tightly within the POR. The prime contractor appoints an Engineering Review Board (ERB) that coordinates directly with the PMO to define program deliverables and to monitor and control the forward motion of individual activities. The ERB works closely with the PMO's RMB to account for risks from activities and to track milestone deliverables against the overall Risk Management and Project Management Plans.

As a major transportation agency puts it, the art of SE is to resolve uncertainty early in the project lifecycle by establishing project scope, defining quantifiable requirements, and using incremental development strategies to mitigate the risk of unreliable work estimates.[34] The ERB within the POR accomplishes this by implementing SE using a classic "v-diagram" similar to the one shown below:

[34] Source: FHA01 in references. The POR uses a similar model.

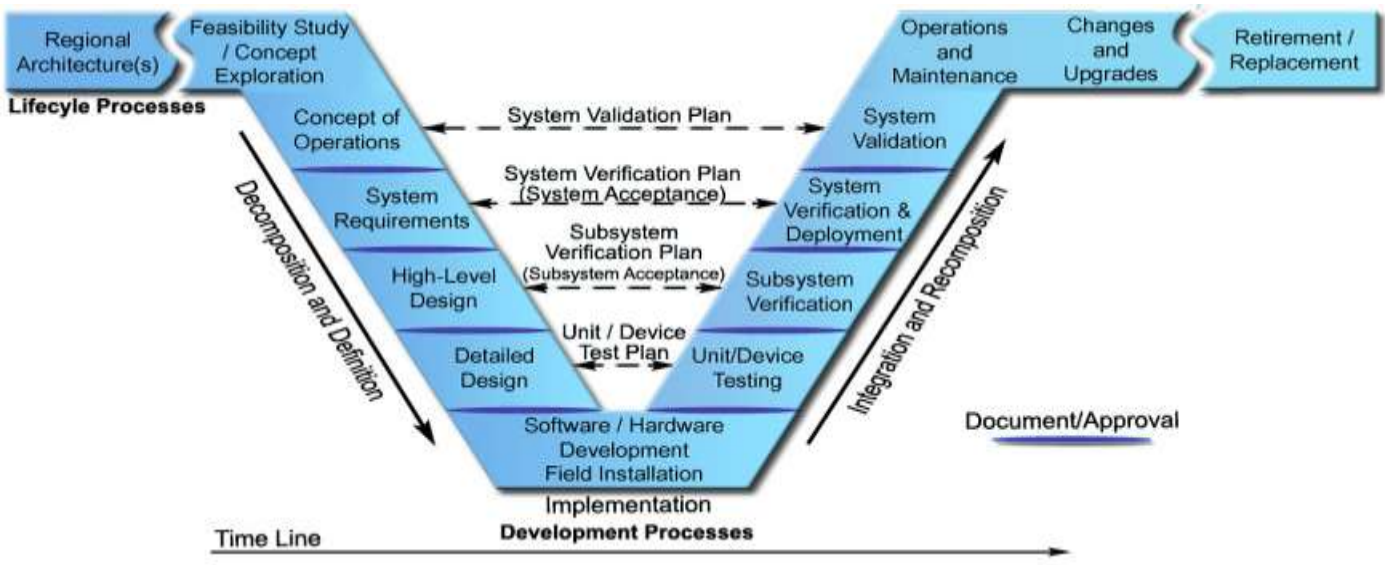


Figure 3: Systems Engineering V-Diagram[35]

The POR's SELC minimizes risk by ensuring that each work activity within the POR results in a well engineered, reliable, and quality-oriented deliverable.

The POR could improve its overall RM by clearly communicating its chosen security controls to its software development team(s). Under the current SE model, the Quality Assurance (QA) group verifies Development compliance to IA controls during system testing. However, this can lead to longer production cycles if IA compliance faltered during the Development phase.

2.4.3.3 Sustainment Level

In order to demonstrate due care and fiduciary responsibility, the POR's senior management team must ensure that released and production-quality systems maintain their operational integrity. As the U.S. Computer Emergency Response Team (US-CERT) has demonstrated, threats to production systems evolve constantly as new system vulnerabilities are discovered by attackers.[36] To maintain the POR's readiness within its Production and COOP sites, system administrators adhere strictly to guidance provided by the DISA Enclave Security Technical Implementation Guide (STIG) to keep risk at acceptable levels (DISA-STIG-E, p 17):

- Ensure that all security-related patches are applied in conjunction with US-CERT notifications.
- Create and maintain documented security patch management processes and procedures.
- Require all workstations have authorized security patches applied automatically.
- Test security patches in a non-production environment prior to deployment into the Production

[35] Source: FHA01 in references. The V-Diagram used by the POR is proprietary information and cannot be shown.

[36] US-CERT works closely with DoD to evaluate and prioritize emerging computer threats. See http://www.us-cert.gov/current/ for the list of current activities and vulnerabilities (accessed: February 18, 2011).

enclave.

By applying sound RM methodologies at the PMO, SE, and Sustainment levels, the POR demonstrates its commitment to reducing and controlling the cost of unmitigated risks.

2.4.4 Risk Management and Cost Control

RM reduces cost by removing or minimizing uncertainties within an endeavor. The DoD specifies that RM should be implemented throughout a project or program's lifecycle, and the POR accomplishes this by injecting RM at all phases of its SELC.

2.4.4.1 Risk Cost

Yalian Zhang (2009) posits that "risk cost" should be evaluated as a separate line item within the organization's accounting structure. Both realized risks and the measures to control those risks have costs associated with them. For RM to be effective, the cost of any single risk control should not exceed the cost of the risk being mitigated, transferred, or avoided. Moreover, Zhang argues that risk management cost and risk occurrence cost are inversely correlated; the higher the one, the lower the other. (This assumption holds true only when risks have been properly identified and evaluated; an improperly executed RM plan can be quite expensive while failing to reduce risk substantially.) Thus, the goal of an RM program is to identify risks fully and to implement only those controls that cost-effectively reduce risks to an acceptable level.

2.4.4.2 Risk Cost and the PMI Approach

The PMI specifies a formula for determining the funding necessary to manage risk within a project: multiply the probability of a risk occurrence by the estimated cost of that occurrence (PMI, p 301). Consider the risk to a computer data center if a major flood occurs. First, the cost impact of the risk occurrence is calculated: the cost of lost revenue, the cost of facility repairs, and the estimated effects upon employee staffing; this cost is called the Single Loss Expectancy (SLE). Then the probability is calculated that the data center will be flooded during a single year (in this case, by using public records of flood occurrences); this becomes the Annual Rate of Occurrence (ARO). By multiplying the SLE by the ARO, one gets the annual risk impact (the Annual Loss Expectancy, or ALE). In short, the formula for allocating an annual risk management budget is:

Annual Risk Budget (ALE) = Total Expected Loss (SLE) * Probability of Occurrence (ARO)

Assume that the risk's cost impact to the data center is estimated at $1,000,000 for a major flood (this becomes the SLE). Furthermore, assume that public records indicate that such a flood occurs once every forty years. Thus, the probability that the flood will occur in a given year (the ARO) is 1⁄40, or 2.5%. The ALE can be calculated as:

Annual Funding for Data Center Flooding (ALE) = $1,000,000 * .025 = $25,000

In this case, approximately $25,000 should be allocated per year for data center floods. Such an approach has definite weaknesses: using the above example, Management must accept the risk that insufficient funding will be available if a flood occurs prior to the forty year period. However, this approach has definite value when used as a discriminator to determine if an alternative approach (such as purchasing insurance) is cost-effective.

2.4.4.3 Risk Cost and the NIST Approach

Despite the PMI's recommendation, neither NIST nor the DoD currently recommends the ALE approach. NIST SP

800-30 (“Risk Management Guide for Information Technology Systems”) instead recommends that either a qualitative or quantitative cost-benefit analysis should be performed. The purpose of such an analysis is to determine whether and how risk reduction justifies a security control’s implementation. This approach poses the following questions (NIST 800-30, p 37-38):

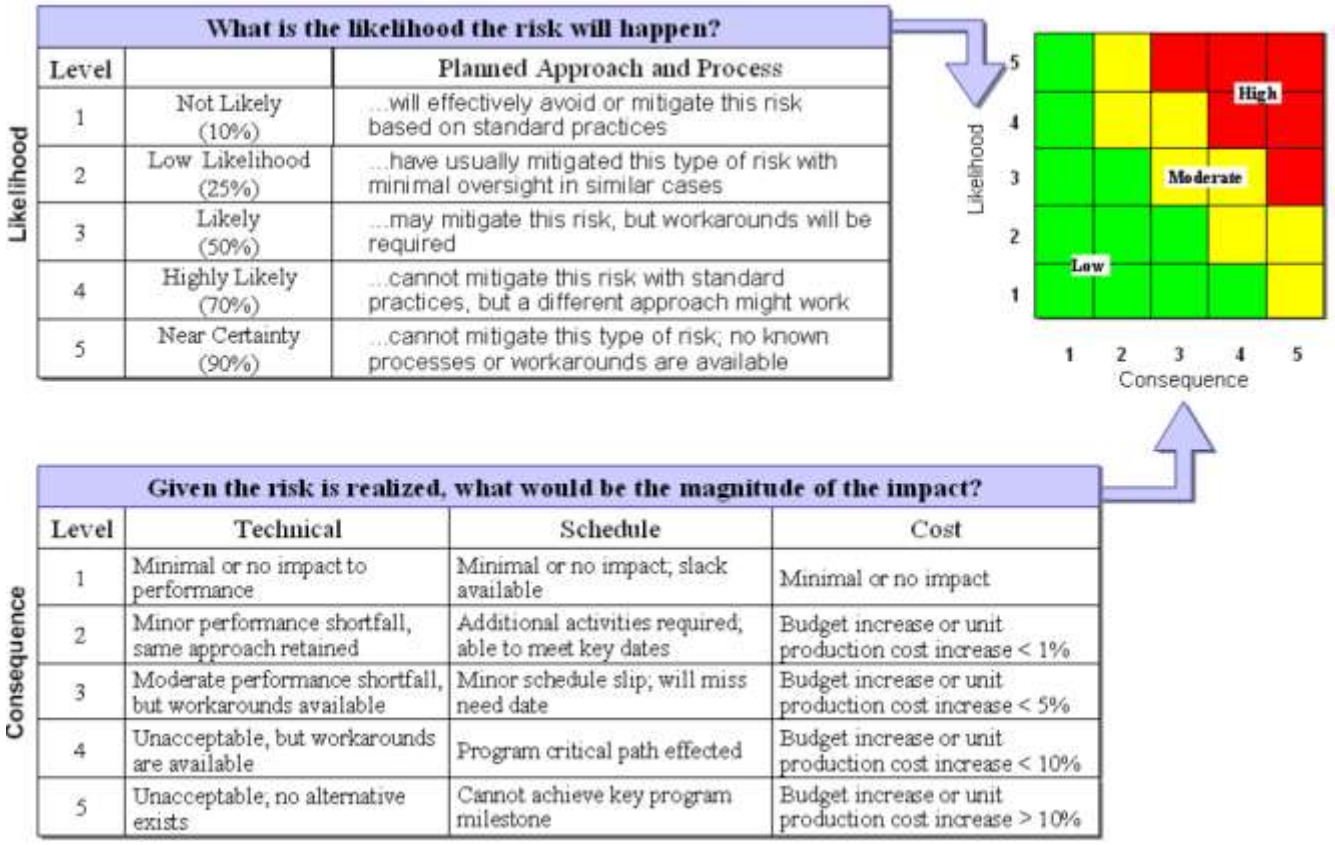
- What is the impact of implementing a new or enhanced control?
- What is the impact of not implementing the new or enhanced control?
- What are the costs of implementing the control? These costs include: necessary hardware or software; impact on production systems; policy and procedure updates; possible new required personnel; and, training / maintenance costs.
- How do the control’s costs and benefits weigh against each other, taking into consideration the criticality of the data or system being protected?

To answer these questions, the risk assessor must fully understand the data and/or systems under review. A Business Impact Analysis (BIA) aids the assessor in coming to this understanding; absent a BIA, the assessor is hard-pressed to determine the criticality of the item under review to the organization’s overall mission.

2.4.4.4 Risk Cost Control

A properly executed RM plan means that management is cognizant of the true costs a risk occurrence would incur. This understanding leads to viable funding requests, which in turn allows Congress to make an informed decision about whether the benefits of the POR justify its ongoing operational costs.

RM planning allows for the prioritization of risk and the allocation of risk controls to where they make the most sense. RM competes for scarce funding resources along with development and sustainment costs; rather than applying risk controls such as computer access locks and manned entry-points indiscriminately, management can see where the greatest potential problems lie and apply funds against those risks that most threaten the POR. The DoD advocates the usage of a simple “Risk Assessment Cube” as shown below:



What is the likelihood the risk will happen?

Level		Planned Approach and Process
1	Not Likely (10%)	...will effectively avoid or mitigate this risk based on standard practices
2	Low Likelihood (25%)	...have usually mitigated this type of risk with minimal oversight in similar cases
3	Likely (50%)	...may mitigate this risk, but workarounds will be required
4	Highly Likely (70%)	...cannot mitigate this risk with standard practices, but a different approach might work
5	Near Certainty (90%)	...cannot mitigate this type of risk; no known processes or workarounds are available

Given the risk is realized, what would be the magnitude of the impact?

Consequence

Level	Technical	Schedule	Cost
1	Minimal or no impact to performance	Minimal or no impact; slack available	Minimal or no impact
2	Minor performance shortfall, same approach retained	Additional activities required; able to meet key dates	Budget increase or unit production cost increase < 1%
3	Moderate performance shortfall, but workarounds available	Minor schedule slip; will miss need date	Budget increase or unit production cost increase < 5%
4	Unacceptable, but workarounds are available	Program critical path effected	Budget increase or unit production cost increase < 10%
5	Unacceptable; no alternative exists	Cannot achieve key program milestone	Budget increase or unit production cost increase > 10%

Figure 4: DoD's Risk Assessment Cube[37]

By focusing resources against those risks identified in the "High Consequence / High Likelihood" zone (the red zone in the chart) overall risk can be kept to an acceptable level while RM funds are used most effectively.

[37] Source: "PMA-234 Risk Management Plan (RMP)," *U.S. Navy Naval Air Systems Command*, March 1, 2008. Available at http://www.navair.navy.mil/doing_business/open_solicitations/uploads/N00019-08-R-0101/080229_PMA-234_RMP.pdf (accessed: February 3, 2011).

3.0 Recommendations

The POR has demonstrated its ability to succeed as a long-running operational program in a challenging environment by taking the proactive approaches summarized above. The POR has excelled by virtue of its solid engineering practices, high-quality employment and ethical decision-making policies, and RM program. Implementation of the improvements recommended by this paper would enable the POR to sustain and augment its proven efficacy. This section elaborates on the aforementioned recommendations and estimates each one's impact on the POR's scope, time, and cost baselines.

3.1 Implement Strong Authentication for all Computer Logins

3.1.1 Overview

As noted in Section 2.2.2.1, many POR workstations lack strong (two-factor) authentication.[10] All workstations should require a SmartCard[38] for login. Currently, POR employees (both government and contractor) are each issued a CAC[11] by the DoD; these CACs could be used as SmartCards for login to local workstations.

Credit is due to the POR for already requiring CAC login to secure systems. Even for workstations that use only user ID and password, the CAC must be used for the POR employee to access most DoD Web sites (and any remote system). Universal requirement of a CAC for initial workstation login would use CACs to their full potential.

3.1.2 Cost Estimate

Implementing SmartCard login to all of the POR's workstations would require its own formal project.[39] However, this project would demand little monetary outlay because the POR can standardize and reuse the SmartCard support technology already in place. The following table outlines the high-level steps:

Table 1: SmartCard Login for All Workstations

Step	Benefit for POR	Cost / Impact	Risk	Mitigation
Planning	Defines goals and stakeholders	15 days	Key subsystems undetected	Run network scans to inventory all networks and workstations
Build Team	Supports implementation	One resource from each major POR Team Member	Team has insufficient resources / skill	Require Microsoft Certification Assign each

[38] SmartCards can be thought of as small, tamperproof computers offering both a central-processing unit (CPU) and data storage (both volatile and non-volatile). Source: Jan De Clercq, "SmartCards," *Microsoft TechNet*, http://technet.microsoft.com/en-us/library/dd277362.aspx (accessed: February 2, 2011).

[39] "The SmartCard Deployment Cookbook," *Microsoft TechNet*, http://technet.microsoft.com/en-us/library/dd277386.aspx (accessed: February 2, 2011).

Step	Benefit for POR	Cost / Impact	Risk	Mitigation
		(contractors / government). Assume around 15 people on the team.	levels	inventoried network segment to the Team Member controlling it
Functional Specifications	Provides detailed specifications on SmartCard and card reader hardware selection	Zero; CAC already selected and workstations are already SmartCard enabled		
User Directory Configuration	Associates public certificates from the CAC to the POR's user directory	20 days	CAC certificates from existing users are not included (denial of login)	Use CAC certificates from DoD access site
Pilot	Allows POR to validate that workstation login using CAC occurs seamlessly	20 days	Users cannot login to workstations	Use Group Policy Objects (GPOs) to enable SmartCard login only selectively and provide Help Desk support

By implementing SmartCard login for all workstations, the POR would realize immediate cost savings by reducing Help Desk support calls for password resets. Also, reduction of the risk of unauthorized logins would decrease the overall attack surface available to malicious insiders.

3.2 Integrate Vendor Employment Policies and POR Publications

3.2.1 Overview

Section 2.3.2.2 identified one problem inherent to any situation in which multiple vendors must work together in a secured environment: ensuring that each vendor's employment policies are well-understood and align to authoritative directives. Section 2.3.3 asks how the POR can ensure that publications depending upon an authoritative policy source are kept updated as the policies backing them evolve. In the POR's case, that would include keeping its overall RM Plan aligned with the guidance provided by the J53's ERM Plan. This section suggests a technical solution to both of these problems.

3.2.2 Cost Estimate

COTS vendors offering records management toolsets compliant to DoD 5015.02-STD ("Electronic Records Management Software Applications Design Criteria Standard") were asked to present a scalable solution

addressing the following requirements:

1. *Allow master checklists / correlation lists to be created (such as based on CNSSI 1253 or DoD NIST SP 800-53)*. These checklists would correspond to the master policies from DoD and DLA as well as pertinent Federal laws and regulations.
2. *Ingest unstructured documents and allows analysts to map document sections to the created master checklists / correlation lists.* Analysts would receive softcopies of contractor and subcontractor employment policies and use these softcopies for ingestion. The individual employment policies would be mapped to the federal, DoD, and DLA authoritative drivers.
3. *Generate gap analysis reports and provide Key Performance Indicator (KPI) dashboards via a Web presentation.* The PMO would use this capability to publish "health scorecards" explaining how well the program as a whole complies with employment policy mandates.

Table 2: Cost estimates to integrate Vendor Employment Policies with POR

Product	Features	Cost (Year 1)	Maintenance	Cost (Year 5)
Hewlett-Packard TRIM 7[40]	Integrates into numerous existing document management systems and client applications Highly customizable Certified for Classified data storage	100 base seats (GSA pricing): $63,500.00 Recommended consulting engagement to create "Model Office": $125,000.00 *Total: $188,500.00*	$15,000.00 / year	$248,500.00
Feith Document Database 8[41]	Flexible document capture method Supports workflow throughout document lifecycle Fine-grained permission support Full lifecycle management	25 base seats for BridgeLogiQ platform: $100,000.00 Estimated consulting costs to setup full solution: $250,000.00 *Total: $350,000*	$20,000.00 / year (software) $50,000.00 / year (professional services)	$630,000.00
Systemware Records Manager 1.1.0[42]	Advanced document management systems Used throughout DoD Complete solution package	100 base seats (GSA pricing): $360,000.00 Recommended consulting engagement: $90,000.00 *Total: $450,000*	$72,000.00 / year	$738,000.00

Vendors furnished the above estimates to give a rough idea of overall costs. To move forward on this project, the PMO must issue an RFQ to the vendor community in accordance with (IAW) the Defense Federal Acquisition Regulations System (DFARS). The presented solutions are all fully-featured COTS offerings. Each RFQ can be used

[40] Source: Customized estimate from HP Software (DoD Sales), February 7, 2011. See www.hp.com for company information.

[41] Source: Customized estimate from Feith Systems and Software, February 18, 2011. See www.feith.com for company information.

[42] Source: Customized estimate from Systemware, February 24, 2011. See http://www.systemware.com/ecm-products/records-management for company and product information.

to establish a trusted competency baseline for all records management, including:

1. A policy-driven foundation for information governance,
2. Tight integration into standard DoD desktop application environments,
3. Integrated and automated data archival process, and
4. Powerful search capabilities for regulatory compliance and litigation discovery.

A full discussion of these offerings is beyond the scope of this paper, but the PMO can and should perform additional analysis on this topic.

3.3 Identify all User Identity Usage within the POR

3.3.1 Overview

Section 2.3.4 identified a problem common to all enterprises: that of identifying all uses of an employee's identity within the corporate network (especially when that employee is leaving). Disabling an employee's network account can sometimes lead to mysterious application failures when that employee's account has been used to run common services or scheduled batch jobs. While the POR is technologically vendor-agnostic, a significant portion of the POR's network runs under Microsoft Windows Active Directory. Thus, this section identifies COTS tools that can aid in the management of account usage within the Active Directory environment.

3.3.2 Cost Estimate

Costs were collected from three COTS tool vendors; each vendor was asked to present a scalable solution that:

1. Tracks all account usages within the Active Directory network (approximately 20 domains and 1,800 users).[43]
2. Allows system administrators to automate service account management.
3. Provides Key Performance Indicator (KPI) reports indicating account usage.

Table 3: Cost estimates to identity all User Identity Usage with POR

Product	Features	Cost (Year 1)	Maintenance	Cost (Year 5)
Namescape mPowertools and rDirectory[44]	Web-based control panel (rDirectory) Track changes across the directory (rDirectory) Integrated reporting (mPowertools)	rDirectory (1800 seats): $9,900.00 mPowertools (20 seats): $15,980.00 40 hours consulting: $10,000 *Total: $35,880.00*	$2000.00 / year (20% of rDirectory cost)	$43,880.00
ScriptLogic Desktop	Centralized management of Active Directory	Active Administrator (100 seats): $825.00	$10,530.00 (Desktop Authority seat licenses	$68,475.00

[43] Source for estimated domains and workstations: POR Security Officer, January 25, 2011.

[44] Source: Customized estimate from Namespace Corporation (Federal Sales), February 15, 2011. See www.namescape.com for company information.

Product	Features	Cost (Year 1)	Maintenance	Cost (Year 5)
Authority and Active Administrator[45]	Desktop Authority provides full control over user workstations (would handle account tracking) No consulting offered	Desktop Authority (1800 seats): $10,530.00 Estimated learning / deployment: $15,000 *Total: $26,355.00*	valid for one year)	
Tools4Ever[46] User Management Resource Administrator	Delegation of user account management Provision of user self-service with auditing Workflow management (would handle employee termination and account tracking)	1800 seats: $9,900.00 Consulting services (40 hours): $7,500.00 *Total: $17,400*	$1,980.00 / year (1800 seats)	$25,320.00

As in Section 3.2.2, vendors furnished the above estimates to give a rough idea of overall costs. To move forward on this project, the PMO must issue an RFQ to the vendor community IAW the DFARS. Each of the offerings can be used for far more than simply tracking account usage across the POR's installed desktop baseline. The PMO should review these solutions against its existing set of desktop management systems to determine how implementation of a comprehensive Active Directory management solution could consolidate costs and increase centralized efficiency.

3.4 Communicate Security Controls to Development

3.4.1 Overview

Section 2.4.3 (particularly Section 2.4.3.2) demonstrates the POR's commitment to RM throughout the entire SELC but identifies an area for improvement: selected security controls should be communicated more clearly to the different software development team(s). As a DoD program, the POR has mapped its IA requirements to DoD Instruction 8500.02.[47] For software development teams to produce compliant and secure deliverables, security controls need to be mapped to the specific POR requirements that drive these deliverables, as shown in the flow below:

[45] Source: Active Administrator customized estimate from ScriptLogic (Federal Sales), February 7, 2011. Desktop Authority pricing / maintenance from reseller, February 15, 2011 (Programmer's Paradise, http://www.programmers.com/ppi_us/Product.aspx?skupart=SP5 01).

[46] Source: Customized estimate from Tools4Ever Corporation (Federal Sales), February 4, 2011. See www.tools4ever.com for company information.

[47] As of October, 2009, DoD is moving toward closer integration with NIST Special Publication 800-53 ("Security Controls") and away from DODI 8500.02. The POR still uses the 8500.02 security control mappings.

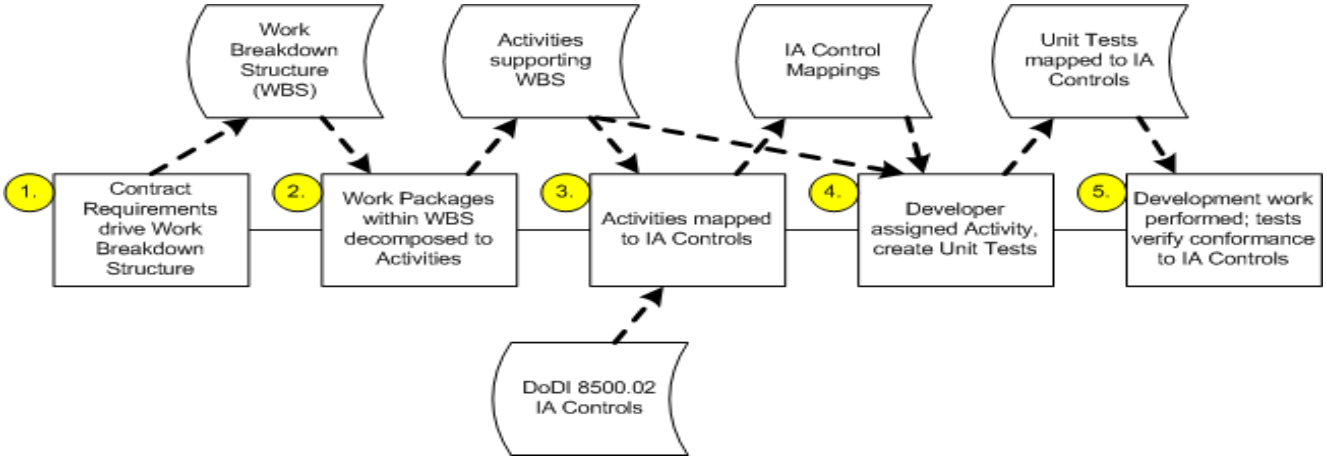


Figure 5: Development IA Control Mapping[48]

By ensuring that development activities and unit tests are mapped to relevant IA controls, the POR can achieve two positive results:

1. Developers are made aware of the security controls that POR deliverables must include and support.
2. Overall costs are reduced by ensuring that security controls are always applied as part of the SE Development cycle rather than simply being verified after development has been completed.

3.4.2 Cost Estimate

Because the POR's existing QA management plan already accounts for IA compliance, the primary expenses of implementing this improvement would stem from:

1. The review of existing development activities to ensure that the project plan is current;
2. Share and training Development staff in IA controls and test case development; and,
3. Integrate QA test cases with Development test cases to ensure full IA control coverage.

Table 4: Integrate Security Controls with Development

Step	Benefit for POR	Cost / Impact	Risk	Mitigation
Work Breakdown Structure (WBS) and Activities	Maps contract requirements to specific deliverables	Zero (WBS and Activities are already created)	N/A	N/A
Map IA Controls to Activities	Eliminates reactive cost to apply IA Controls after	One dedicated SO to work with Project Management – 20	Bottleneck to existing activity development	Continue current activity development

[48] Drawing by the author.

Step	Benefit for POR	Cost / Impact	Risk	Mitigation
	development	days		unchanged
Assign IA Control Mappings as part of Activity assignments	Ensures security and operational concerns are understood	Develop training material (2 team members, 5 days) Train development teams (2 team member, 5 days)	Development is unable to create unit tests	SO works with teams to answer questions and update training documents
Integrate to Quality Assurance (QA)	Separation of duties (IA compliance verification separated from Development)	10 days training (all teams, 2 days per team)	QA test cases may not match Development	Integrate test case development efforts between QA and Development to create one set of tests

By implementing this improvement to the current SE model, the POR will achieve cost savings by decreasing overall testing and verification time for individual software deliverables.

4.0 Summary

This paper examined how an operational program of record (the POR) within the DLA is using specific IA techniques to solve real business problems and achieve cost reduction while simultaneously maintaining quality control. The specific methodologies employed by the POR to secure its overall program environment include a number of best-practices defined at both the Department (DoD) and the Agency (DLA) levels.

Far from being an unproductive overhead cost, IA instead performs the same function as HR, Accounting, and Management; that is, IA enables an organization to accomplish its mission and to achieve its objectives. Additionally, both the DoD and the DLA are held to stringent IA requirements to ensure that the Nation's critical defense infrastructure is maintained with a high level of confidentiality, integrity, and availability.

The POR creates a "hard shell" around itself by using OPSEC and defense in depth. The POR's facilities feature controlled entry and exit points and increasingly specific defenses both logical (such as layered workstation protections) and physical (increasingly secured areas within each facility). The POR ensures availability to its customers by implementing redundant sites with aggressive RTO and RPO requirements. The combination of these defenses provides the production-ready security posture that the DoD demands.

The POR realizes that a motivated and educated workforce is essential to its mission. This paper explored how the POR's employment practices support this workforce throughout the employment lifecycle. From a contractual level, the POR requires that the implementing prime contractor (and all subcontractors) follow explicit employment guidelines. Once employed, employees receive tailored SAT based on their job roles and classifications. The POR actively supports its employees in expanding their areas of competency, thus ensuring that the expertise necessary for ongoing and expanding program operations can be provided as much as possible by in-house resources. Ongoing SAT ensures that these employees understand the changing threat landscape and helps the POR's management team to receive the support it needs to identify and mitigate threats.

Due to the sensitive nature of the data being processed on a daily basis, ethical decision-making is critical to every DoD program. The military nature of the DLA and the POR means that both classified and unclassified information must be handled and in some cases this data must be orchestrated together. While it is hard to overstate the primary role that OPSEC fills in providing security protection, numerous cases show that, in the end, a human being provides the first and last lines of defense in INFOSEC. Ethical training encourages that human being to work on behalf of the organization instead of against it. The POR's SAT includes a strong dose of ethics: from proper handling of PII, to users' responsibilities in reporting observed violations.

Ultimately, the POR is judged based on how well it executes its mission. Missions can fail for many reasons; improper planning, external problems, even bad luck. At the end of the day, however, the POR must succeed. The POR addresses risk according to a sound RM plan that is an integral part of its overall SELC. The POR's PMO identifies and mitigates risks using all of the approved DoD techniques: avoidance by taking an alternate approach; controlling (mitigating) the cause or consequences of an identified risk; transferring the risk by purchasing insurance; or, assuming the risk and quantifying its impact and probability in order for appropriate funding to be reserved.

In short, the POR's effective use of an IA program ensures that the nation receives the best possible value for expended public funds; additionally, the POR's IA program leads to a stronger workforce, a more empowered external customer base, and a more agile response capability to support the Warfighter.

Appendix A: Recommendations by Cost and Priority

Recommendations: By Cost

Of the four recommendations made by this paper, two pertain to product acquisitions and two do not. The product acquisition suggestions are associated with estimated dollar amounts, while the non-product acquisition suggestions are associated with estimated time impact. This paper puts the product acquisition suggestions first; however, this does not imply that the actual cost of the non-product acquisition suggestions will be greater or less than the product acquisition suggestions.

Table 5: Recommendations by Cost

Item	Overview	Reasoning	Costs
Implement Strong Authentication for all Computer Login	Ensure that all workstation logins use strong (two-factor) authentication and require a SmartCard for login.	Currently, POR employees (both government and contractor) are each issued a CAC, which could be used as the SmartCard for login to local workstations as well.	1 PM resource for 55 days. 15 team member resources for 40 days.
Communicate Security Controls to Development	Ensure that all development teams are aware of the security controls which their software deliverables must support and to which these deliverables must adhere.	While security control verification occurs during the QA testing phases, ensuring that developers are aware of these controls can reduce costs by preventing rework.	1 SO for 40 days 2 technical writers for 5 days 2 trainers for 20 days 10 days training at 5 persons per day; 50 days total.
Identify all user identity usage within the POR	Ensure that, as employees leave the POR, their account usage within the POR's computer network is identified.	When employee user accounts are used to run batch jobs on individual workstations, these batch jobs must be identified and updated to use a different account.	Low: $25,320.00 Mid: $43,880.00 High: $68,475.00
Integrate Vendor Employment Policies and POR Publications	Ensure that all vendors' employment policies are well-understood and align to authoritative directives, and ingest each vendor's policies into a centralized database.	DoD 5015.02-STD defines a set of approved records-management software that can perform gap analysis between vendor policies and applicable laws and regulations.	Low: $248,500.00 Mid: $630,000.00 High: $738,000.00

Recommendations: By Priority

This section prioritizes recommendations in the order that they should be implemented by the PMO.

Table 6: Recommendations by Priority

Item	Overview	Reasoning
Implement Strong Authentication for all Computer Login	Ensure that all workstation logins use strong (two-factor) authentication and require a SmartCard for login.	Currently, POR employees (both government and contractor) are each issued a CAC, which could be used as the SmartCard for login to local workstations as well.
Identify all user identity usage within the POR	Ensure that, as employees leave the POR, their account usage within the POR's computer network is identified.	When employee user accounts are used to run batch jobs on individual workstations, these batch jobs must be identified and updated to use a different account.
Communicate Security Controls to Development	Ensure that all development teams are aware of the security controls which their software deliverables must support and to which these deliverables must adhere.	While security control verification occurs during the QA testing phases, ensuring that developers are aware of these controls can reduce costs by preventing rework.
Integrate Vendor Employment Policies and POR Publications	Ensure that all vendors' employment policies are well-understood and align to authoritative directives, and ingest each vendor's policies into a centralized database.	DoD 5015.02-STD defines a set of approved records-management software that can perform gap analysis between vendor policies and applicable laws and regulations.

Appendix B: Acronyms and Abbreviations

ACL	Access Control List
ALE	Annual Loss Expectancy
ARO	Annual Rate of Occurrence
AUP	Acceptable Use Policy
BIA	Business Impact Analysis
CAC	Common Access Card
CJCS	Chairman, Joint Chiefs of Staff
CNSS	The Committee for National Security Systems
CNSSI	Committee for National Security Systems Instruction
COOP	Continuity of Operations
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CSA	Cognizant Security Agency
DD	Department of Defense (Form)
DISA	Defense Information Systems Agency
DAC	Discretionary Access Controls
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
EEOC	Equal Employment Opportunity Commission
ERB	Engineering Review Board
ERM	Enterprise Risk Management
FSO	Field Security Officer
GPO	Group Policy Object
IA	Information Assurance
IA&ISP	Information Assurance and Industrial Security Plan
IASE	Information Assurance Support Environment
IBM	International Business Machines

INFOSEC	Information Security
IOC	Initial Operating Capability
IP	Intellectual Property
IRCA	Immigration Reform and Control Act of 1986
ISSA	Information Systems Security Association
IT	Information Technology
J53	Risk Assessment & Process Improvement Division (DLA)
JTF-GNO	Joint Task Force – Global Network Operations
KO	Contract Officer
MAC	Mandatory Access Controls
NIST	National Institute of Standards and Technology
No.	Number
OPSEC	Operational Security
PII	Personally Identifiable Information
PIN	Personal Identification Number
PMBOK®	Project Management Body of Knowledge
PM	Program (or Project) Manager
PMI	Project Management Institute
PMO	Program (or Project) Management Office
POR	The DLA Program of Record serving as the Use Case for this paper
QA	Quality Assurance
RFQ	Request for Quotation (Firm Fixed Price contract)
RM	Risk Management
RMB	Risk Management Board
ROI	Return on Investment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAT	Security Awareness Training
SCA	The Service Contract Act of 1965
SE	Systems Engineering

SELC	Systems Engineering Lifecycle
SF	Standard Form
SLA	Service Level Agreement
SLE	Single Loss Expectancy
SME	Subject Matter Expert
SO	Security Officer
SP	Special Publication (NIST)
U.S.	United States
US-CERT	U.S. Computer Emergency Response Team
USB	Universal Serial Bus
USCYBERCOM	U.S. Cyber Command

Reference List

[ALLEN10] Allen TT. 2010. Introduction to Engineering Statistics and Lean Sigma: Statistical Quality. London: Springer-Verlag. 576 p.

[BOS09] Bosworth S, Kabay ME, Whyne E, editors. 2009. Computer Security Handbook. 5th ed. Hoboken (NJ): John Wiley & Sons, Inc. 2035 p.

[CLARKW-87] Clark D, Wilson D. 1987. A Comparison of Commercial and Military Computer Security Policies. IEEE Symposium on Security and Privacy: p 184-194.

[CNSSI-4009] Committee on National Security Systems. CNSSI Instruction No. 4009: National Information Assurance (IA) Glossary. April 26, 2009. <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>. Accessed: February 4, 2011.

[DISA-STIG-E] Defense Information Systems Agency. March 10, 2008. Enclave Security Technical Implementation Guide. Version 4, Release 2. <http://iase.disa.mil/stigs/stig/enclave_stigv4r2.pdf>. Accessed: February 20, 2011.

[DOD-RMG] Department of Defense. August, 2006. Risk Management Guide for DoD Acquisition. 6th ed. (Version 1.0). <http://www.dau.mil/pubs/gdbks/risk_management.asp>. Accessed: February 24, 2011.

[DODD-1440] Department of Defense. May 21, 1987. (Certified current as of November 21, 2003.) DoD Directive 1440.1: The DoD Civilian Equal Employment Opportunity (EEO) Program. <http://www.dtic.mil/whs/directives/corres/pdf/144001p.pdf>. Accessed: February 24, 2011.

[DODD-5205] Department of Defense. March 6, 2006. DoD Directive 5205.02: DoD Operations Security (OPSEC) Program. <http://www.dtic.mil/whs/directives/corres/pdf/520502p.pdf>. Accessed: February 3, 2011.

[DODD-5500] Department of Defense. November 29, 2007. DoD Directive 5500.07: Standards of Conduct. <http://www.dod.gov/dodgc/defense_ethics/ethics_regulation/dir550007.pdf>. Accessed: February 12, 2011.

[DODD-8570] Department of Defense. December 19, 2005 (incorporating changes through April 20, 2010). DoD Directive 8570.01-M: Information Assurance Workforce Improvement Program. <http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>. Accessed: February 12, 2011.

[DODI-1400] Department of Defense. September 26, 2006. DoD Instruction 1400.20: DoD Program for Stability of Civilian Employment. <http://www.cpms.osd.mil/care/docs/dod1400.pdf>. Accessed: February 5, 2011.

[DODI-5000.02] Department of Defense. December 8, 2008. DoD Instruction 5000.02: Operation of the Defense Acquisition System. <http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf>. Accessed: February 19, 2011.

[DODM-4245.7] Department of Defense. DoD Manual 4245.7-M. Transition from Development to Production. <https://acc.dau.mil/adl/en-US/25653/file/55201/DoD%204245.7-M.pdf>. Accessed: February 19, 2011.

[DODM-5205] Department of Defense. November 3, 2008. DoD Manual 5205.02-M: DoD Operations Security (OPSEC) Program Manual. <http://www.dtic.mil/whs/directives/corres/pdf/520502m.pdf>. Accessed: February 18, 2011.

[DODM-5220] Department of Defense. February 28, 2006. DoD Manual 5220.22-M: National Industrial Security Program Operating Manual. <http://www.usaid.gov/policy/ads/500/d522022m.pdf>. Accessed: February 18, 2011.

[DODI-8500] Department of Defense. February 6, 2003. DoD Instruction 8500.02: Information Assurance (IA) Implementation. <http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>. Accessed: February 18, 2011.

[FHA01] Federal Highway Administration. Systems Engineering for Intelligent Transportation Systems: Section 3. FHA Online Publications. <http://ops.fhwa.dot.gov/publications/seitsguide/section3.htm>. Accessed: February 2, 2011.

[NIST 800-30] Stoneburner G, Goguen A, Feringa A. Special Publication 800-30: Risk Management Guide for Information Technology Systems [Internet]. Gaithersburg (MD) [cited February 16, 2011]. Available from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. 55 p.

[PMI] Project Management Institute. 2008. A Guide to the Project Management Body of Knowledge (PMBOK®). 4th ed. Newtown Square (PA): PMI.

[PL08] Public Law. Title 8 U.S. Code, Pts. 1101: Immigration Reform and Control Act of 1986.

[PL41] Public Law. Title 41 U.S. Code, Pts. 351: Service Contract Act of 1965 (January, 2006 ed.)

[STE03] Stephenson PR, ed. 2009. Information Security Essentials (Section 3). Auerbach Publishing, ISBN 978-1-4398-0030-0. 684 p.

[ZHANG] Zhang Y. May 2009. A Study on Risk Cost Management. Int J of Bus and Mgmt 4(5): 145-148.