SYM-AM-16-039

PROCEEDINGS
OF THE
THIRTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

WEDNESDAY SESSIONS
VOLUME I

Issues With Access to Acquisition Data & Information in the Department of Defense: Policy & Practice

Megan McKernan, Defense Research Analyst, RAND
Jessie Riposo, Senior Operations Researcher, RAND

Published April 30, 2016

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Business & Public Policy at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

Panel 8. Data Policies, Procedures, & Access: Illuminating How Acquisition Information Moves Within the Department to Support Analysis & Decision Making

Wednesday, May 4, 2016	
3:30 p.m. – 5:00 p.m.	**Chair: Mark Krzysko,** Deputy Director, Acquisition Resources and Analysis, OUSD (AT&L) **Discussant: Ralph DiCicco,** Acquisition Chief Information Officer (CIO), United States Air Force ***Issues With Access to Acquisition Data & Information in the Department of Defense: Policy & Practice*** Megan McKernan, Defense Research Analyst, RAND Jessie Riposo, Senior Operations Researcher, RAND ***Issues With Access to Acquisition Data & Information in the Department of Defense: Doing Data Right in Weapon System Acquisition*** Nancy Moore, Senior Management Scientist, RAND Megan McKernan, Defense Research Analyst, RAND

Issues With Access to Acquisition Data & Information in the Department of Defense: Policy & Practice

Megan McKernan—is a Defense Research Analyst at RAND. McKernan has more than 10 years of experience conducting DoD acquisition analyses. She is currently co-leading research examining acquisition data sharing in the DoD. McKernan has also conducted analyses on other defense acquisition topics: tailoring the acquisition process, program manager tenure, and root causes of Nunn-McCurdy unit cost breaches. She uses a variety of methods in conducting research, including case studies, interviews, and literature reviews. She holds an MA in international trade and investment policy from George Washington University and a BA in economics from William Smith College. [mckernan@rand.org]

Jessie Riposo—is a Senior Operations Researcher at RAND, with over a decade of experience in research and analysis with a specialty in Defense Acquisition and Planning, Programming, and Budgeting. Since 2003, Riposo has led and participated in projects in support of the USD(AT&L), U.S. Navy, UK MoD, and the Australian DoD. Riposo's projects have covered reviews of domestic and foreign acquisition programs, Department acquisition policy and industrial base, personnel, and policy assessments. Riposo has applied a variety of quantitative and qualitative tools, such as statistical analyses, mathematical modeling, surveys, and interviews in her analyses. [riposo@rand.org]

Other co-contributors from RAND: Jeffrey A. Drezner, Douglas Shontz, Geoffrey McGovern, Daniel Tremblay, Clifford Grammich, Jerry M. Sollinger, Jason Kumar

Abstract

Acquisition data underpin the management and oversight of the U.S. defense acquisition portfolio. However, balancing security and transparency has been an ongoing challenge. Some acquisition professionals are not getting the data they need to perform their assigned duties or are not getting the data and information in an efficient manner. To help guide the Office of the Secretary of Defense (OSD) in addressing these problems, the RAND Corporation identified access problems at the OSD level—including those organizations that require access to data and information to support the OSD, such as analytic support federally funded research and development centers and direct support contractors—and evaluated the role of policy in determining access. The study also involved a limited review of how data are shared between the OSD and military departments. Issues with access to acquisition data and information in the Department of Defense (DoD) finds that the process for gaining access to data is inefficient and may not provide access to the best data to support analysis, and that OSD analytic groups and support contractors face particular challenges in gaining access to data. Given the inherent complexity in securing data and sharing data, any solutions to problems associated with data sharing must be well thought out to avoid the multitude of unintended consequences that could arise.

Introduction

Acquisition data are vast and include such information as the cost of weapon systems (both procurement and operations), technical performance, contracts and contractor performance, and program decision memoranda. These data are critical to the management and oversight of the $1.5 trillion portfolio of major weapon programs by the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD[AT&L]; GAO, 2014, p. 3). Data collection and analysis enable the Department of Defense (DoD) to track acquisition program and system performance and ensure that progress is being made toward such institutional goals as achieving efficiency in defense acquisition and delivering weapon systems to the field on time and on budget.

Many organizations or groups need access to this information for a variety of purposes (e.g., management, oversight, analysis, and administrative). These organizations

include various offices of the DoD, federally funded research and development centers (FFRDCs), university-affiliated research centers (UARCs), and a range of support contractors. For example, an FFRDC may need cost and schedule information to determine whether a weapon system was delivered on time and within budget. Or a support contractor may be responsible for managing a centralized information system for the DoD that contains information about specific procurement programs. Note that that situation does not include classified data, which is not a topic of this report.[1]

However, these organizations may have difficulty getting access to these data. Some examples of the types of issues identified by individuals within DoD offices include the following:

- "It took me three months, multiple e-mails, and phone calls to get a one-hour meeting with five SES [DoD senior executive service–level employees] to view data that might be proprietary."
- "Each access account I create is like five touch points between an email, phone call, their POC, certificate handling, vetting. It's a lot of work."
- "If there are dozens of support contractors and dozens of prime contractors and I have to get an NDA [nondisclosure agreement] for each support contractor and prime contractor combination, it's a lot of work."
- Examples of the types of issues identified by FFRDC, UARC, and direct support contractors include
- "The sponsor has to have access, then request a download of several documents I need, then transfer the data to me."
- "I couldn't get access because I didn't have a .mil e-mail address."

In some cases, the information may be the intellectual property of a commercial firm. Sometimes such information is designated *proprietary*. This information requires the permission of the firm that owns the information to use it. The process of getting permission to use the information can be time-consuming, may never yield permission, or is simply too onerous. An example of the third possibility is a database that has proprietary information from many firms, requiring support contractors to sign NDAs with each firm, which could number many dozens and take a very long time.

The Office of the Secretary of Defense (OSD) asked the RAND National Defense Research Institute to identify the problems and challenges associated with sharing unclassified information and to investigate the role of policies and practices with such sharing in the first phase of two analyses on acquisition data (Riposo et al., 2015). In the second phase, RAND was asked to evaluate how marking and labeling Controlled Unclassified Information (CUI) procedures, practices, and security policy affect access to acquisition oversight data (McKernan et al., 2016). We will present the approaches, findings, and options for improvement for both analyses.

---

[1] Classified information is any information designated by the U.S. government for restricted dissemination or distribution. Information so designated falls into various categories depending on the degree of harm its unauthorized release may cause. This report does not deal with classified information.

Phase 1 Approach

We pursued a three-pronged approach for the first phase of this research with the objective of defining and evaluating any data-sharing problems. The first part of the approach was a policy review. We began by reviewing DoD directives, instructions, manuals, and guides, along with executive orders, legislation, and regulations concerning information management. The objective of the review was to develop a framework for understanding what governs information sharing in DoD acquisition. As part of this search, we also looked at a limited number of key federal policies that might affect data sharing within the DoD.

We then met with individuals within OSD to discuss information sharing, which is the second part of our approach. We used these discussions to help identify information-sharing practices and issues associated with data access and releasability. The discussions also helped us identify relevant policies and practices. We selected a sample of offices within OUSD(AT&L) to reflect a variety of roles in the acquisition process. We spoke with data owners, maintainers, users, and individuals involved with the governance of information. We categorized the offices represented in the sample by their missions and roles. This step led to three main categories of OSD offices:

- functional and subject-matter experts
- Overarching Integrated Project Team/Defense Acquisition Board (OIPT/DAB) review offices
- analysis offices

Within the OSD, the functional and subject-matter experts mainly work within a specialty (e.g., testing, cost, systems engineering, contracts, earned value). Those in the OIPT offices are primarily responsible for direct interaction with acquisition programs to review portfolio status and program readiness as programs move through the acquisition process. The analysis offices conduct a variety of crosscutting analyses in defense acquisition. The offices that fall into these categories appear in Table 1. We also interviewed service-level acquisition personnel to determine the role that the services play in DoD data sharing.

Our goal for the interviews was to collect the following information regarding interviewees' data sharing and practices:

- role in the acquisition process
- data needed to perform one's job
- how data are handled, obtained, and provided to others
- data access or release problems
- data-sharing recommendations

Table 1. Offices With Roles in the Acquisition Process

Office Category	Offices
Functional and Subject-Matter Experts	• OUSD(AT&L) Performance Assessments and Root Cause Analyses (PARCA) Earned Value Management (EVM) • OSD Cost Assessment and Program Evaluation (CAPE) • OUSD(AT&L) Human Capital Initiative (HCI) • OUSD(AT&L) Defense Procurement and Acquisition Policy (DPAP) • OUSD(AT&L) Developmental Test and Evaluation (DT) • OUSD(AT&L) Systems Engineering (SE)
OIPT/DAB Review Offices	• OUSD(AT&L) Deputy Assistant Secretary of Defense (DASD) Tactical Warfare Systems (TWS) • OUSD(AT&L) DASD Space, Strategic and Intelligence Systems (SSI) • OUSD(AT&L) DASD Command, Control, Communication, Cyber and Business Systems (C3CB)
Analysis Offices	• OUSD(AT&L) Acquisition Resources and Analysis (ARA) • OUSD(AT&L) Defense Acquisition University (DAU) • DPAP • FFRDCs • OUSD(AT&L) PARCA (outside EVM)

The final part of our three-pronged approach for phase 1 involved conducting two case studies to illuminate key issues and challenges associated with data access. Both reflect (or embody) the perception of several key data access issues. The first case study examines the use of proprietary information (PROPIN) in acquisition, with a particular focus on earned value data. The second looks at the various central data repositories that OSD maintains and uses. More specifically, the focus was on the background, benefits, and problems associated with these repositories. During our introductory interviews, we heard about problems with using, managing, and accessing PROPIN due to the need to involve direct support contractors in the collection and analysis of these data. Such relationships require the use of NDAs to help prime contractors and subcontractors protect their information. Both case studies are informed by the interview results and policy analysis.

Phase 2 Approach

During the second phase of this analysis on acquisition data, we evaluated how marking and labeling CUI procedures, practices, and security policy affect access to acquisition oversight data. Our work for this phase of research on managing and handling acquisition data within the DoD included policy analysis, structured discussions with government personnel, and a literature review to further understand and evaluate proprietary information sharing, the origins of commonly used acquisition labels, and how security policy affects the management of two acquisition information management systems within the OUSD(AT&L). We executed our work through three main tasks.

- **Identify and evaluate options to improve nongovernment employee access to proprietary information:** We continued to explore the source of the problems identified in our earlier research with sharing proprietary data among the government, contractor-originators who are providing the acquisition information, and other nongovernment entities such as federally funded research and development centers (FFRDCs), Systems Engineering and Technical Assistance (SETA) support, and information technology (IT) support contractors who are supporting the government. We developed a range of options for improving direct access for nongovernment employees to proprietary data and documented the options that the OUSD(AT&L) is pursuing to improve sharing. We characterized the options and their advantages and disadvantages and assessed implementation strategies for them.

- **Characterize commonly used data markings that support acquisition decision-making and oversight and identify the origins of those markings:** We focused on CUI labels that are commonly used by DoD government and nongovernment employees in the acquisition process. We identified their basis in law and policy and determined whether the policy prescriptions they provide for data labeling and access are clear and consistent and accord with OUSD(AT&L) goals. OUSD(AT&L) decision-making and oversight is intimately connected to acquisition data access, research, and analysis. Whether these data are available for timely, actionable decision-making partially depends on the type of data, the data control system, and the ability of data users to properly identify and label data, and if necessary, challenge improperly marked data.
- **Describe how DoD security policies, processes, and procedures affect OUSD(AT&L)'s ability to provide efficient and secure access to acquisition data:** This task involved multiple steps. First, we collected policies that affect information security and defense acquisition data for two information systems within the OUSD(AT&L)—Acquisition Information Repository (AIR) and the Defense Acquisition Management Information Retrieval (DAMIR) information systems. Second, we described the security policy environment for managing these information systems (e.g., who owns these policies and what topics they discuss). Third, we described and summarized the information security policy and identified how particular policies affect the OUSD(AT&L)'s ability to provide access to acquisition data and manage acquisition data.

Phase 1 Findings and Recommendations

- **The process for gaining access to data is inefficient and may not provide access to the best data to support analysis.** Government personnel and those supporting the government sometimes do not get their first choice of data, and even that data may take a long time to receive. They may be forced to use alternative sources, which often have data of lower quality, which might be dated and thus less accurate, or be subject to a number of caveats. While the consequences of these limitations are undocumented and difficult to assess and quantify, the results of these analyses can be inferior, incomplete, or misleading.
- **Two groups of people face particular challenges in gaining access to data: OSD analytic groups and support contractors.** OSD analytic groups often do not have access to the originators of the data, which precludes them from going to the primary source. They also tend to have poor visibility of all viable data sources, which encourages inefficient data-seeking practices. Direct support contractors have problems similar to OSD analysts, but these problems can be compounded by laws, regulations, and policy that restrict access to certain types of information (especially nontechnical proprietary data that originate and are labeled outside the government), which introduces extreme inefficiencies. Support contractors require special permissions to view nontechnical proprietary data.
- **Difficulty in gaining access occurs for several reasons:**
    - Data access policy is highly decentralized, not well known, and subject to a wide range of interpretation.

- The markings for unclassified information play a significant role in access. The owner or creator of a document determines what protections or markings are required. However, marking criteria are not always clear or consistently applied. In fact, management and handling procedures for many commonly used markings are not clearly described anywhere. Once marked, getting the labels changed can be difficult. When information is not marked, the burden of handling decisions is placed on the receiver of the information.
- Institutional and cultural barriers inhibit sharing. The stove-piped structure of the DoD limits visibility and sharing of data and information. Institutional structure and bureaucratic incentives to restrict data access are exacerbated by policy and guidance to protect information. The result is a strong conservative bias in labeling and a reluctance to share. A lack of trust and established relationships can hinder sharing.

Options for Improving Data Sharing

The variety of identified problems may be addressed in many ways. Each potential option requires further analysis and investigation. We offer initial thoughts to deal with the issue of access to proprietary data, as well as the general confusion regarding policy.

Options to Address Problem of Proprietary Data Access

There are several potential options to resolve the problem of access to proprietary data.

- The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) could seek additional billets and insource any functions that require access to proprietary data. However, this would require Office of Personnel Management and congressional support.
- USD(AT&L) could seek relief through a reallocation of billets to functions that currently require access to proprietary information. This would require cross-organizational prioritization, a difficult process.
- General access could be established for all direct support contractors. This would require legislative or contractual changes. Current legislation, Title 10 U.S. Code, Section 129d, allows litigation support contractors to view proprietary information. Similar legislation might be pursued for all support contractors.
- Alternatively, additional contractual language could be placed on all DoD acquisition contracts granting support contractors restricted access to their data. The direct support contractors who receive the data would have to demonstrate company firewalls, training, personal agreements, and need to know akin to those for classified information.
- The government could seek an alternative ruling on the nondisclosure requirements, whereby blanket nondisclosure agreements could be signed between the government and a direct support organization, or a company and a direct support organization to cover multiple tasks.

Each of these options would require further analysis and coordination with Office of the General Counsel and Defense Procurement and Acquisition Policy (and Congress in the first and third options).

Options to Address Policy Confusion

There are also several options to address the confusion regarding policy.

- OUSD(AT&L) could create and maintain a central, authoritative online resource that references all relevant guidance on information management, handling, access, and release for acquisition data. This would require identifying the relevant policy and posting new policies as they become available.
- However, an online resource may not address the issue of the workforce having a general lack of expertise and insight regarding the existing policy and guidance. To cope with this problem, OUSD(AT&L) could also consider providing additional training for its staff on the identification and protection of data. This could be an annual online training for all OUSD(AT&L) staff and contractors.
- In areas where conflicting interpretations of guidance are particularly problematic, such as with For Official Use Only (FOUO) and proprietary information, additional guidance about how to determine whether information is FOUO or proprietary in the first place would be helpful. The guidance should provide specific examples of information that is considered protected, guidelines for determining whether specific information qualifies, and details regarding handling procedures for this information, to include access privileges.
- Directives and incentives could be established so that markings that appear to be incorrect are challenged and not taken only on a company or individual's claim. If more-detailed determination guidance is available, it could be used to assess the validity of a marking. A process should be in place for challenging markings, and it should be exercised.

There are important reasons for restricting access that require balancing control with granting more access. In information assurance and security policy, there is an understanding that no individual should have unfettered access to all data. Given the inherent complexity in securing data and sharing data, any solutions to problems associated with data sharing must be well thought out to avoid the multitude of unintended consequences that could arise.

Phase 2 Findings and Recommendations

Proprietary Information (PROPIN)

PROPIN is a special class of CUI that relates to information and data developed by a private entity but shared with the government. Substantial confusion exists within the DoD about what information is truly proprietary, who can have access to it, and how to grant access when needed. Despite the fact that some policies attempt to define PROPIN and handling restrictions, no single source describes the processes and procedures for dealing with this type of information. Rather, a patchwork of law, regulation, and policy govern it, some of which is clear, but some of which is less so. This hinders the DoD's use of contractors, restricts information flow, and limits analyses.

DoD personnel are confused about who can access PROPIN. Information so characterized generally can be treated like all other CUI, meaning all government personnel can be granted access (Treanor, 1999). This access is enabled by virtue of the fact that the government has obtained the information under a lawful requirement. Further, federal employees who improperly use PROPIN can be fired and/or prosecuted. In addition,

employees with a security clearance sign a blanket nondisclosure agreement (NDA) between the employee and the government. However, many government personnel are not familiar with this longstanding practice and are reluctant to share information with other government personnel because of concerns about violating an unknown law or regulation. In addition, procedures for nongovernment personnel to gain access vary widely. Federal law (10 U.S.C. 2320) specifically addresses support contractor access to technical data provided, but that law does not address nontechnical proprietary information supplied by contractor-originators. Consequently, DoD personnel often grapple with access issues among government and nongovernment personnel because of the lack of clear guidance about who can access what information—and what information constitutes PROPIN.

Ultimately, the company submitting the information to the government is responsible for asserting that certain portions are proprietary, but the government recipient is responsible for determining whether to accept that assertion and maintaining the "proprietary" label.[2] In other words, if the responsible government official determines the information is not proprietary, the government person is under no obligation to go back to the company (originator) to disclose the information within the government to a support contractor. If the government person wants to publicly disclose the information in response to a FOIA request, then the government person would have to notify the company (originator). However, true PROPIN can only be disclosed within the government to support contractors (and now FFRDC employees) when a one-to-one (i.e., between each individual at the support contractor/FFRDC and each company or program originating data) NDA has been executed.

The government distinguishes between contractors, generally, and the special contractual relationship established with federally funded research and development centers (FFRDCs).[3] In the past, the special relationship has meant that FFRDC personnel could be granted access to information directly by government personnel, or by signing a single, blanket NDA between the employee and the government, allowing them access to proprietary information in the course of their government-related work. But federal law does not specifically define what an FFRDC is or how to grant FFRDC personnel access to PROPIN. Nontechnical PROPIN is not specifically defined in statute, and courts have stated that what is truly proprietary is determined on a case-by-case basis under FOIA Exemption 4. Generally, the disclosure of the information must present the potential for a company's

---

[2] This statement is based on the researchers' understanding of current practices.

[3] FFRDCs have a unique relationship with the government because they have access beyond that which is common to the normal contractual relationship. They are free from organizational conflicts of interest. Also, it is not the government's intent that an FFRDC use its privileged information or access to installations equipment and real property to compete with the private sector. Finally, FFRDCs are meant to be independent research institutions characterized by objectivity. According to 48 C.F.R. 35.017 (a.k.a. FAR 35.017), "An FFRDC, in order to discharge its responsibilities to the sponsoring agency, has access, beyond that which is common to the normal contractual relationship, to Government and supplier data, including sensitive and proprietary data, and to employees and installations equipment and real property. The FFRDC is required to conduct its business in a manner befitting its special relationship with the Government, to operate in the public interest with objectivity and independence, to be free from organizational conflicts of interest, and to have full disclosure of its affairs to the sponsoring agency. It is not the Government's intent that an FFRDC use its privileged information or access to installations equipment and real property to compete with the private sector."

competitive position to be injured by a competing company (Department of Justice, 2009, p. 305).

Recent DoD interpretations of policy and statute—specifically the Trade Secrets Act (18 U.S.C. 1905)—have changed how FFRDCs are treated with respect to NDAs, resulting in an inefficient and ineffective process of securing them. Specifically, FFRDCs are now required to obtain an NDA between each contractor-originator of data in a system and each FFRDC employee who needs access—referred to in this report as "one-to-one" NDAs. Previously, FFRDC employees could sign a single, blanket NDA with the DoD to enable access to all needed information.

The RAND Corporation operates three FFRDCs: Project AIR FORCE, the Arroyo Research Center, and the National Defense Research Institute. Therefore, we have an interest in FFRDC access to data. We believe that our results are valid independent of that interest, and we have firsthand experience with the struggles of DoD personnel managing data and access.

Commonly Used CUI Data Markings

The current set of CUI labels and guidance states that only information which requires protection by Federal Regulation or government-wide policy can be considered CUI. In other words, a marking that does not originate from a protection established by law or government-wide policy should not be employed. We identified nine data labels commonly used to indicate that the information contained in a document or database requires some type of special handling or restriction. Those nine labels are

- Business Sensitive
- Competition Sensitive
- For Official Use Only
- Pre-Decisional
- Proprietary
- Source Selection Sensitive
- Technical Distribution Statements
- DoD Only
- Government Only

Some of these labels are governed by well-established policies that reflect current understanding of the law and regulatory environment for data protection and data sharing. Others are legacy markings and practices that were not aligned with draft CUI policy at the time this report was written. We were unable to find any single document collecting and describing all these labels; the lack of a single such document contributes to the general confusion surrounding them. It is difficult for government personnel to know how data can be shared. A result of this situation is the likely over-labeling and mislabeling of CUI material. Although we found that many of the most commonly used CUI labels do have a basis in law or policy, labels may not be understood in practice, used properly, or have clear handling procedures.

Consequently, data may not be used to inform, improve, and strengthen the DoD's acquisition functions. Bottlenecks, risk aversion, and fear of releasing otherwise protected data can restrict legitimate access and data sharing, both within the government and between the government and select partners. While the National CUI program being

established by the National Archives will help provide much-needed clarifications, it is unclear when this program will be finalized within the DoD.

Implications of DoD Security Policies for Two OUSD(AT&L) Acquisition Data Information Systems

Information security policies directly affect the access and utility of acquisition databases. The current information security environment does not establish a consistent framework for managing information systems. This makes it difficult for government employees to know how to comply with regulations; find funds and the technical capabilities to implement new policies; develop ways to evaluate costs and benefits of new policies and determine exceptions; and know how to identify, mark, and protect CUI. The impact of these challenges is a potential delay in accessing acquisition data by both government and nongovernment employees, which in turn may result in lower quality analyses or decisions based on incomplete information.

We used the Acquisition Information Repository (AIR) and Defense Acquisition Management Information Retrieval (DAMIR) OUSD(AT&L) acquisition data information systems as case studies to examine the implications of implementing security policies. AIR provides one central location for all Major Defense Acquisition Program (MDAP) and Major Automated Information System (MAIS) acquisition documents to support oversight and decision-making.[4] DAMIR fulfills several key functions, including reporting, storage, quality assurance, analysis, oversight, and tracking cost, schedule, and performance of major acquisition programs.[5] AIR largely represents the unstructured data problem, while DAMIR represents the challenges associated with structured data that both pull from and feed into other information systems.

A multitude of security policies affect management and operation of these systems. We identified about two dozen executive orders, laws, directives, instructions, operating guides, and other policies that affect AIR and DAMIR, some of which cover similar material. The AIR information managers have created a set of business rules based on their interpretation of those policies. For instance, according to DoD (2012) Manual 5200.01, volume 4, “The [government] originator of a document is responsible for determining at origination whether the information may qualify for CUI status, and if so, for applying the appropriate CUI markings” (p. 9). The information managers for AIR have interpreted this policy guidance from USD(I) to mean that the originators of the information being uploaded to AIR (e.g., the services and other OSD offices) are responsible for appropriately marking the information in AIR even though the AIR managers have noticed some inconsistency in the marking of the documents across documents types. The AIR managers attribute this inconsistency to the variety of security classification guides being used to mark documents by the originators. Also, there is no process for ensuring that up-to-date marking conventions are followed for each document uploaded to AIR. Management and use of AIR

[4] AIR is a document repository that contains specific program documents (reports, certifications) used to inform acquisition decision-making and oversight.

[5] DAMIR has both unclassified and classified versions. It supports the generation, distribution, and archiving of Selected Acquisition Reports (SARs) as well as information supporting the Defense Executive Acquisition System (DAES) process. It also includes higher-level earned value management data. Unlike AIR, DAMIR is structured data that users can combine and analyze in multiple ways serving multiple functions.

are complicated by the need to access it on an IT system approved through Defense Security Service inspection, use a .mil e-mail address associated with a Common Access Card (CAC), and have approval through a government sponsor, who provides the rationale for granting a user access to AIR for a specific purpose. In addition, the permissions process is separate from the sensitivity of documents stored in AIR.

DAMIR is hosted by the Joint Service Provider, which only partially resides within the OUSD (AT&L). External hosting separates operational and security management and creates the possibility of a disconnect between the business case for data use and security policies. In other words, the cost of the security may be high while the perceived benefits may be low. Understanding the business case (or use) for DAMIR is critical to maintaining security without unduly limiting the utility of the system for users. Security policies also inhibit system improvement, which requires code changes and upgrades. A recent determination that real data cannot be used for testing required additional programming work to invent data to test the system. The lack of actual data for testing makes determining whether a new database capability will ultimately work a speculative exercise.

Several years ago a security policy requiring accounts that have not been used in a 30-day period to be disabled significantly affected DAMIR. Many DAMIR users, including congressional staff and FFRDC analysts, log in infrequently (i.e., when new SAR or DAES reports come out) rather than routinely. The policy resulted in the suspension of accounts, which meant the DAMIR team had to re-register about 30% of 4,000 active user accounts initially after the policy was enforced. The DAMIR team continued to have significant problems for several months in re-activating inactive accounts.

Implementing new policies within DAMIR (which has more than 1.5 million lines of code) is also challenging. DAMIR was stood-up under different security-related policies, and adapting its structure, programming, and business rules to accommodate new policies entails substantial effort. Furthermore, there is no up-to-date security architecture document because architecture and security policy governing DAMIR have evolved independently. Similarly, new interpretations of existing policies have consequences. For example, a new interpretation[6] of what potentially constitutes personally identifiable information (PII) caused the DAMIR management team to conduct a formal assessment of how individual privacy is being addressed in DAMIR due to the potential existence of PII in DAMIR.

CUI Marking and the Security Policy Environment

Overall, the current environment in which acquisition data are protected and shared can be characterized by many organizations promulgating policy on overlapping and interrelated topics, policies that are relatively new and change frequently, and an ill-defined CUI policy. Furthermore, security policies tend to be one-size-fits-all, which does not reflect the unique characteristics of each system. Those who originate the policies do not fund their implementation, meaning that a new or changed policy is effectively an unfunded requirement for system managers. This situation creates a number of issues for information system managers. First, it is difficult to know exactly what is required to comply with the

[6] The interpretation was based on the reissue of DoD Directive (DoDD) 5400.11 that updated the established policies and assigned responsibilities of the DoD Privacy Program pursuant to section 552a of Title 5, U.S.C. (also known and referred to in this directive as “The Privacy Act” and Office of Management and Budget [OMB] Circular No. A-130).

numerous applicable policies. Second, managers have to find the funds to comply when policies change. Third, considerable confusion surrounds the identification and marking of CUI. This environment, which is causing a lot of inefficiency and many workarounds to solve problems, creates a managerial problem for the OUSD(AT&L).

The overall effect of these problems almost certainly has a cost, though this cost is difficult to quantify. Government and nongovernment users of both DAMIR and AIR may, for example, simply seek to conduct analyses with other, less insightful data, or without data at all. No system, however, tracks the effects or costs of DAMIR and AIR (or any other information system) compliance with security policy. The cumulative effects of security policy requirements may exceed what is currently documented in the management of these two acquisition information systems. In other words, the effect of compliance actions on other information systems and user behavior can have a cascading effect; the problem is likely much larger than what has been documented here.

What the DoD Can Do to Improve the Situation

Proprietary Data

We suggest[7] that the Federal Acquisition Regulation (FAR) FFRDC provisions could be used as a basis for a DoD decision that FFRDCs are exempt from the relatively new one-to-one NDA requirement created by a change in DoD interpretation of the Trade Secrets Act, or could be covered by a single, blanket NDA with the DoD.[8] Office of Federal Procurement Policy staff suggested in a meeting with the authors of this report that the DoD Office of the General Counsel (OGC) was taking an overly restrictive view of the FAR FFRDC provisions. For non-FFRDC contractors, we also recommend that the DoD consider the following:

- Creating a DFARS provision that would cover nontechnical data,[9] possibly with a blanket NDA requirement
- Proposing a new legislative provision covering all nongovernment personnel similar to 10 U.S.C. 129d, which allows litigation support contractors access to "commercial, financial, or proprietary information" without a nondisclosure agreement
- Proposing a legislative amendment to 10 U.S.C. 2320, which allows access to technical data for providing advice or technical assistance to the government, that would include financial and management data

Regulatory and legislative changes both carry drawbacks. The DoD can propose changes to the DFARS without congressional action and presidential approval, but changing

---

[7] Our recommendations are designed to increase access to sensitive data for analysis. As a party that has long analyzed such data, organizations such as RAND (an FFRDC) would, of course, benefit from such actions, and we understand readers may view our recommendations accordingly. Regardless, we trust our research can advance broader discussion of how the DoD can improve oversight of its acquisition programs.

[8] A blanket NDA would be an NDA between an organization and another organization, versus the current requirement of a one-to-one NDA between an individual and a contractor-originator of data.

[9] As noted above, 10 U.S.C. 2320 specifically addresses technical data, so we are only discussing nontechnical data.

the DFARS might not adequately include previous PROPIN designations because a new clause would only affect contractors who presently have active DoD contracts. Changing the law is even more problematic because it requires congressional action and presidential approval, takes approximately two or more years, and may not even result in a change or could result in unwanted changes.

CUI Markings and Labels

A more robust, central program for CUI data labeling, access, and management (including monitoring and challenging document originators) may help facilitate a smoother sharing and protection of CUI within the DoD. The DoD should also train its workforce on the new CUI labeling procedures when they are released and implemented by the DoD. Given that no central reference, institutional structure, or authority exists for defining and establishing proper handling procedures for CUI, we recommend that a function and reference be established within the OUSD(AT&L) for both technical and nontechnical acquisition data.

Security Policy

The problem that needs to be solved with respect to security policy is the clear mismatch of responsibility, authority, and accountability among the organizations that issue security policy and manage or host the information systems. We offer several recommendations oriented at addressing this problem.

First, we suggest using existing information requirements to document how security policies are affecting the management of information systems. While there are many anecdotes about difficulties in implementing security policy for AIR and DAMIR, these are not documented in a central location or updated over time. By documenting difficulties, including resources used to implement various policies, the OUSD(AT&L) would better understand how security policies are affecting their systems and whether a better balance between security and business cases[10] is being achieved.

Second, we suggest that a function be established within the OUSD(AT&L) to review information security policies, de-conflict them, reduce duplication, ensure consistency, and identify gaps for all acquisition data collected and used within the OUSD(AT&L). This function would be responsible for communicating with the OUSD(AT&L) information-system managers in order to have a greater understanding of the inefficiencies in implementing security policy. This function (or working group) should include all relevant stakeholders so as represent both security and mission perspectives.

Third, a single individual should be designated with responsibility for implementing security strategy for a given information system. This individual, the AO, could work with the policy originator to ensure appropriate interpretation and application of policy. For the OUSD(AT&L) information systems, we believe that the AO should be selected based on knowledge of the mission area (i.e., a subject matter expert). The goal is to have someone

---

[10] Enterprise Information within OUSD(AT&L)/ARA is responsible for "providing leadership timely access to accurate, authoritative and reliable data supporting acquisition oversight, analysis, and decision-making." EI needs to fulfill its mission with limited resources, so it must balance the business case for adding new capability to its information systems (DAMIR and AIR) with what is being mandated for it to implement for adequate security of its information systems.

who is familiar with the business case for a system to be more involved in the daily operations of that system and to track security policy changes and implementation.

Fourth, the requirement that each information system have and maintain a security strategy should be used as an opportunity to ensure an appropriate balance between security risk, business case, and the use case[11] for each information system. The security strategy should be updated as policies, threats, or system use change, providing a consistent framework over time to evaluate the balance between risk and utility.

Finally, implementation of security policy should be appropriately resourced. The issuing organization should assess required resources as part of policy design, and provide at least some funding to address needed technical changes to the information systems. Similarly, the organizations managing information systems should identify resources to address implementation of security policy as part of the security strategy it maintains.

References

Legal Information Institute. (n.d.) 10 U.S. Code § 2320—Rights in technical data. Cornell University Law School. Retrieved from http://www.law.cornell.edu/uscode/text/10/2320

McKernan, M., Riposo, J., Drezner, J. A., McGovern, G., Shontz, D., & Grammich, C. (2016). *Issues with access to acquisition data and information in the Department of Defense: A closer look at the origins and implementation of controlled unclassified information labels and security policy* (RR-1476-OSD). Santa Monica, CA: RAND.

Riposo, J., McKernan, M., Drezner, J. A., McGovern, G., Tremblay, D., Kumar, J., & Sollinger, J. M. (2015). *Issues with access to acquisition data and information in the Department of Defense: Policy and practice* (RR-880-OSD). Santa Monica, CA: RAND. Retrieved from http://www.rand.org/pubs/research_reports/RR880.html

Treanor, W. M. (1999, April 5). *Applicability of Trade Secrets Act to intra-governmental exchange of regulatory information* [Memorandum]. Office of Legal Counsel, DoJ.

18 U.S.C. § 1905, Disclosure of Confidential Information Generally (2014).

DoD. (2012, February 24). *DoD Information Security Program: Controlled unclassified information (CUI)* (Manual 5200.01, Vol. 4). Washington, DC: Author.

Department of Justice. (2009). *Guide to the Freedom of Information Act.* Washington, DC: Author. Retrieved from http://www.justice.gov/oip/doj-guide-freedom-information-act-0

GAO. (2014, March). *Defense acquisitions: Assessments of selected weapon programs* (GAO-14-340SP). Washington, DC: Author.

[11] Interactions between the users of DAMIR/AIR and system owners that enables the user to achieve the goal of adequate access to acquisition data.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CA 93943

www.acquisitionresearch.net