

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

Megan McKernan, Jessie Riposo,
Jeffrey A. Drezner, Geoffrey McGovern,
Douglas Shontz, Clifford A. Grammich



For more information on this publication, visit www.rand.org/t/RR1476

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-0-8330-9596-1

Published by the RAND Corporation, Santa Monica, Calif.

© Copyright 2016 RAND Corporation

RAND® is a registered trademark.

Cover: iStock.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of its research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Support RAND

Make a tax-deductible charitable contribution at
www.rand.org/giving/contribute

www.rand.org

Preface

Acquisition data play a critical role in the management of the U.S. Department of Defense's (DoD's) portfolio of weapon systems. Management and sharing of these data are subject to the interaction and interpretation of a large quantity of laws, regulations, and policies; Controlled Unclassified Information (CUI) labels; and DoD culture, among other influences. This complex environment for acquisition data leads to a host of inefficiencies for those who manage and utilize these data.

The Office of the Secretary of Defense asked RAND to take a closer look at several key sources of inefficiency by evaluating how marking and labeling CUI procedures, practices, and security policies affect access and management of acquisition oversight data. This builds on our earlier work (Riposo et al., 2015, *Issues with Access to Acquisition Data and Information in the Department of Defense: Policy and Practice*) by examining in more detail issues with sharing proprietary information, using CUI labels, and implementing security policy in the Acquisition Information Repository and the Defense Acquisition Management Information Retrieval information systems. This report should be useful to government acquisition professionals, oversight organizations, and, especially, the analytic community.

This research was sponsored by the Office of the Secretary of Defense and conducted within the Acquisition and Technology Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

For more information on the RAND Acquisition and Technology Policy Center, see www.rand.org/nsrd/about/atp or contact the director (contact information is provided on the web page).

Contents

Preface	iii
Figures and Tables	vii
Summary	ix
Acknowledgments	xix
Abbreviations	xxi
 CHAPTER ONE	
Introduction	1
Approach	3
Organization of This Report	4
 CHAPTER TWO	
Proprietary Information: Clarifying and Creating Confusion	5
What Is Truly Proprietary Information?	6
Who Can Access PROPIN?	10
Determining How to Grant Access to PROPIN	12
How DoD Is Addressing PROPIN	15
 CHAPTER THREE	
Origins and Meaning of Commonly Used Controlled Unclassified Information Labels	
on Acquisition Data	17
Guiding Questions and Choice of Labels	18
Overview of Commonly Used Acquisition Data Labels	19
Findings	28
 CHAPTER FOUR	
Security Policy and Its Implications for AIR and DAMIR	29
Background	29
Security Policies Identified Through Discussions	31
AIR: Implications and Challenges for Implementing Security Policy	38
DAMIR: Implications and Challenges for Implementing Security Policy	39
Impacts of Security Policies	41
Findings	41

CHAPTER FIVE

Conclusions and Options	45
Proprietary Information.....	45
Origins and Meaning of Commonly Used CUI Acquisition Labels.....	46
Security Policy and Its Implications for AIR and DAMIR	47
Options for Improving the Three OUSD(AT&L) Data Issues	47

APPENDIX

DoD OGC Legal Opinion Dated February 1999	51
--	----

Bibliography	53
---------------------------	----

Figures and Tables

Figures

1.1.	Influences on Access to Acquisition Data.....	2
4.1.	Hierarchy of Organizations That Issue Security Policies.....	32

Tables

3.1.	Common Data Labels, Authorization Basis, and Access Details	20
4.1.	Security Policies Affecting AIR and DAMIR.....	33
4.2.	Basic Characteristics of AIR and DAMIR Information Systems	37
4.3.	Estimated Impacts of Security Policies.....	42
4.4.	Estimated Impacts of General Security Policy Implementation	43

Summary

Background

Data are important to many endeavors, but particularly so in the analysis of U.S. Department of Defense (DoD) acquisition activities. They are essential for determining whether programs are delivering weapon systems that perform as planned for the programmed cost. The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L)) decisionmaking and oversight are intimately connected to data access, as well as to research and analysis that are grounded in acquisition data. Whether these data are available for timely, actionable decisionmaking partially depends on the type of data, the data control system, and the ability of data users to properly identify, label, and, if needed, challenge improperly marked data.

Identifying which unclassified but potentially sensitive data require protection and how to properly protect them through the use of appropriate markings or labels can be problematic. The Controlled Unclassified Information (CUI) program, established by Executive Order 13556,¹ is meant to simplify the labeling of CUI, but the CUI program has not been fully defined and finalized within DoD. CUI has a system of markings to demonstrate that the information is sensitive, but these labels are not always clear, well managed, or well understood. CUI labels need to be used consistently and applied correctly to prevent inefficiencies that lead to wasted resources and potentially poor decisionmaking.

Riposo et al. (2015) found that unclassified acquisition data and related information take several forms (e.g., hard copy, digital repositories, reports and studies).² Many of these forms are exchanged between both government and nongovernment entities throughout the acquisition process. The data and derivative analyses are governed by a system of labels and markings, rules, regulations, and policies. Some of these are well-established policies that reflect current understanding of the law and regulatory environment for data protection and data sharing. Others are outdated, legacy markings and practices that are neither current nor accurately updated.

Existing law and policy allow for some information restrictions based on perceived needs to foster internal deliberations and protect some business interests, among other things; however, data marking and labeling is a process infused with individual judgment and interpreta-

¹ Executive Order 13556 establishes an open and uniform program for managing unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies.

² Jessie Riposo, Megan McKernan, Jeffrey A. Drezner, Geoffrey McGovern, Daniel Tremblay, Jason Kumar, and Jerry M. Sollinger, *Issues with Access to Acquisition Data and Information in the Department of Defense: Policy and Practice*, Santa Monica, Calif.: RAND Corporation, RR-880-OSD, 2015.

tion. The subjectivity and diversity in approaches to data labeling are further magnified and complicated by the sheer number of DoD offices that have a role in creating policy for data handling and management, as well as the number of individuals actually determining which labels to place on the data they use or produce. Ultimately, the researchers found no evidence of a single authoritative source to turn to for questions about how to share data.

DoD acquisition programs and decisionmakers also depend on the support of commercial firms that can produce increasingly complex weapon systems. Understandably, such firms carefully guard the technical and cost information pertaining to the weapon systems they develop. This proprietary information is gained at a high cost and is protected by contractual agreements between vendors and the government. Yet indiscriminate labeling of information as proprietary can complicate program assessment because data labeled as proprietary can be difficult to share with nongovernmental entities assisting DoD (e.g., federally funded research and development centers [FFRDCs], information technology [IT] support, or other contractor support). Proprietary information sometimes takes considerable time to access for nongovernment entities assisting the government and frequently requires negotiations between the contractor originators of the information (prime contractors and subcontractors), the government, and nongovernmental entities assisting the government.

Further complicating the environment in which acquisition data reside is the need to protect information through physical barriers (e.g., the DoD cybersecurity program used to protect and defend DoD information and information technology) defined in a large body of security policy that, like CUI, is subject to interpretation. Information security policy is also written for broad application across DoD (e.g., security policies created by the Undersecretary of Defense for Intelligence [USD(I)] or DoD chief information officer [CIO]) or the government more generally, as in the case of Executive Order 13556, and, therefore, can create an imbalance between security and business cases for information system managers. Finally, OUSD(AT&L) information system managers typically are implementing security policies that originate outside the acquisition domain (e.g., DoDI 8510.01 [*Risk Management Framework {RMF} for DoD Information Technology {IT}*]; DoDI 8520.03 [*Identity Authentication for Information Systems*]; and DISA STIG, Version 3, Release 9 [*DISA Application Security and Development Security Technical Implementation Guide*]).

Purpose and Approach

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 associated with such sharing. We took a phased approach to the analysis. In Riposo et al. (2015), we identified the issues associated with managing and sharing CUI within DoD. In the second phase of this analysis, which this report addresses, we evaluated how marking and labeling CUI procedures, practices, and security policy affect access to acquisition oversight data. To do so, we identified the following three tasks:

- Identify and evaluate options to improve nongovernment employee access to proprietary information.

- Characterize commonly used data markings that support acquisition decisionmaking and oversight and identify the origins of those markings.
- Describe how DoD security policies, processes, and procedures affect OUSD(AT&L)'s ability to provide efficient and secure access to acquisition data.

What We Found

Proprietary Information

Proprietary information (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 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 (e.g., United States Code Title 18, Section 1905 [Trade Secrets Act {TSA}]; DoDI 5230.24; and Exemption 4 of the Freedom of Information Act [FOIA]). This hinders 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 that all government personnel can be granted access.³ 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. Procedures for nongovernment personnel to gain access also vary widely. Federal law specifically addresses access by support contractors to technical data,⁴ 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.⁵ In other words, if the responsible government official determines that the information is not proprietary, the government official is under no obligation to inform the originating company before disclosing the information within the government to a support contractor. If the government official wants to publicly disclose the information in response to a FOIA request, then the official would have to notify the originating company. However, true PROPIN can only be

³ See, e.g., William Michael Treanor, “Applicability of Trade Secrets Act to Intra-Governmental Exchange of Regulatory Information,” Memorandum, Office of Legal Counsel, U.S. Department of Justice, April 5, 1999.

⁴ 10 U.S.C. 2320.

⁵ This statement is based on the researchers' understanding of current practices.

disclosed within the government to support contractors (and now FFRDC employees) when a one-to-one NDA (i.e., an NDA between each individual at the support contractor or FFRDC and each company or program originating data) has been executed.

The government distinguishes between contractors, generally, and the special contractual relationship established with FFRDCs.⁶ In the past, this 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 the employee access to PROPIN in the course of 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 competitive position to be injured by a competing company.⁷

Recent DoD interpretations of policy and statute—specifically the Trade Secrets Act⁸—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 DoD to enable access to all needed information.

The reader is reminded that the RAND Corporation operates three FFRDCs: RAND Project AIR FORCE, RAND Arroyo Center, and the RAND National Defense Research Institute. Therefore, the authors have an interest in FFRDC access to data. However, 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 seven data labels commonly used to indicate that

⁶ 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 for an FFRDC to 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 CFR 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.

⁷ See U.S. Department of Justice, *Department of Justice Guide to the Freedom of Information Act*, Washington, D.C., 2009, p. 305.

⁸ 18 U.S.C. 1905.

the information contained in a document or database requires some type of special handling or restriction:

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

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 when this report was written (January 2016). We were unable to find any single document collecting and describing all of 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 overlabeling 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, be used properly, or have clear handling procedures.

Consequently, data may not be used to inform, improve, and strengthen 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 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, which 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 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 decisionmaking.⁹

⁹ AIR is a document repository that contains specific program documents (reports, certifications) used to inform acquisition decisionmaking and oversight.

DAMIR fulfills several key functions, including reporting, storage, quality assurance, analysis, oversight, and tracking cost, schedule, and performance of major acquisition programs.¹⁰ AIR largely represents the unstructured data problem, while DAMIR represents the challenges associated with pulling or pushing structured data to or from other information systems.

Many security policies affect the management and operation of these systems. We identified approximately 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 Manual 5200.01, Vol. 4 (2012), “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.”¹¹ 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 OSD) 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 document 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 are complicated by the need to access it on an IT system approved through Defense Security Service inspection, using a .mil email address associated with a Common Access Card (CAC), and the need to have access approved by 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 (JSP), which is external to 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 are low. Understanding the business case (or use) for DAMIR is critical to maintain 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 had 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 that the DAMIR team had to reregister about 30 percent of 4,000 active user accounts

¹⁰ 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 Acquisition Executive Summary (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.

¹¹ U.S. Department of Defense Manual 5200.01, Vol. 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)*, Washington, D.C., February 24, 2012, p. 9.

initially after the policy was enforced. The DAMIR team continued to have significant problems for several months in reactivating 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 interpretation¹² of what potentially constitutes personally identifiable information (PII) by JSP, which is the authorizing official (AO) for DAMIR and is therefore responsible for authorizing the system's operation based on achieving and maintaining an acceptable risk posture, directed 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 the system.

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

These problems almost certainly have 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.

¹² The interpretation was based on the reissue of DoD Directive (DoDD) 5400.11, which updated the established policies and assigned responsibilities of the DoD Privacy Program pursuant to section 552a of Title 5, United States Code (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).

What DoD Can Do to Improve the Situation

Proprietary Data

We suggest¹³ 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 that FFRDCs could be covered by a single, blanket NDA with DoD.¹⁴ For non-FFRDC contractors, we also recommend that DoD consider the following actions:

- creating a Defense Federal Acquisition Regulation Supplement (DFARS) provision that would cover nontechnical data,¹⁵ 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. DoD can propose changes to the DFARS without congressional action and presidential approval, but changing 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, would take approximately two or more years, and could result in no change or 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 smoother sharing and protection of CUI within DoD. DoD should also train its workforce on the new CUI labeling procedures when they are released and implemented by 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 (additional responsibility for a currently existing office with experience using a large number of CUI labels in multiple roles) and reference (a central, authoritative online resource that references all relevant guidance on information management, handling, access, and release for acquisition data) be established within OUSD(AT&L) for both technical and nontechnical acquisition data.

¹³ Our recommendations are designed to increase access to sensitive data for analysis. Because RAND, which operates three FFRDCs, has long analyzed such data, RAND itself would, of course, benefit from such actions, and we understand that readers may view our recommendations accordingly. Regardless, we trust that our research can advance broader discussion of how DoD can improve oversight of its acquisition programs.

¹⁴ A blanket NDA would be an NDA between an organization and another organization instead of the current requirement of a one-to-one NDA between an individual and a contractor originator of data.

¹⁵ As noted above, 10 U.S.C. 2320 specifically addresses technical data, so we are discussing only nontechnical 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 for 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, OUSD(AT&L) would better understand how security policies are affecting its systems and whether a better balance between security and business cases¹⁶ is being achieved via these policies.

Second, we suggest that a function be established within OUSD(AT&L) to review information security policies, deconflict them, reduce duplication, ensure consistency, and identify gaps for all acquisition data collected and used within OUSD(AT&L). This function would be responsible for communicating with 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 to 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 who is familiar with the business case for a system to be more involved in the daily operations of that system and 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 among security risk, business case, and the use case¹⁷ 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. Required resources as part of policy design should be assessed, and the appropriate organization should provide at least some funding to address needed technical changes to the information systems.

¹⁶ Enterprise Information (EI) within OUSD(AT&L)/Acquisition Resources and Analysis 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.

¹⁷ The use case covers interactions between the users of DAMIR and AIR and system owners that enable the user to achieve the goal of adequate access to acquisition data.

Acknowledgments

We would like to thank the sponsor of this study: Mark Krzysko, Deputy Director, Acquisition Resources and Analysis (ARA), Enterprise Information, within the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L)). We would also like to thank our project monitors—Jeff Tucker, acquisition visibility capability manager, OUSD(AT&L)/ARA, and Joseph Alfano, former Enterprise Information Studies Program Manager, OUSD(AT&L)/ARA—for their guidance and support throughout this study. Also in OSD, we thank Robert Flowe, OSD Studies and Federally Funded Research and Development Center Management, OUSD(AT&L)/ARA, who provided us with additional background information that informed our analysis. We are also appreciative to Paul DiRenzo, who helped facilitate communication with the Office of Enterprise Information in OUSD(AT&L)/ARA. We would also like to thank the Acquisition Visibility team and everyone else who volunteered their valuable time to describe their points of view to the RAND study team.

We are very grateful to the formal peer reviewers of this document, Debra Schroeder, Edward Keating, William Shelton, and Marilyn May, who helped improve it through their thorough reviews. We also thank Jerry Sollinger, Daniel Tremblay, Christina Dozier, and Maria Falvo for their assistance during this effort.

Finally, we would like to thank the director of the RAND Acquisition and Technology Policy Center, Cynthia Cook, and the associate director, Endy Daehner, for their insightful comments on this research.

Abbreviations

ACAT	Acquisition Category
AIR	Acquisition Information Repository
AO	Authorizing Official
APB	acquisition program baseline
ARA	Acquisition Resources and Analysis
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
ASD(NII)	Assistant Secretary of Defense (Networks and Information Integration)
ATO	Authority to Operate
CAC	Common Access Card
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CND	Computer Network Defense
COR	Contracting Officer's Representative
CUI	Controlled Unclassified Information
DA&M	Director of Administration and Management
DACIMS	Defense Automated Cost Information Management System
DAES	Defense Acquisition Executive Summary
DAMIR	Defense Acquisition Management Information Retrieval
DCMO	Deputy Chief Management Officer
DFARS	Defense Federal Acquisition Regulation Supplement
DISA	Defense Information Systems Agency
DoD	U.S. Department of Defense

DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual
DoD OGC	Department of Defense, Office of General Counsel
DOJ	Department of Justice
DPAP	Defense Procurement and Acquisition Policy
DSS	Defense Security Service
DTIC	Defense Technical Information Center
EI	Enterprise Information
EO	executive order
EVM	Earned Value Management
EVM-CR	Earned Value Management Central Repository
FAR	Federal Acquisition Regulation
FFRDC	federally funded research and development center
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FTE	full-time equivalent
IA	information assurance
IPA	Intergovernmental Personnel Act
IT	information technology
JSP	Joint Service Provider
MAIS	Major Automated Information System
MDAP	Major Defense Acquisition Program
NDA	nondisclosure agreement
NIPRNet	Non-classified Internet Protocol Router Network
OPSEC	operations security
OSD	Office of the Secretary of Defense

OUSD(AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
PARCA	Performance Assessments and Root Cause Analyses
PK	public key
PKI	public key infrastructure
POM	Project Objective Memorandum
PPBE	Planning, Programming, Budgeting, and Execution
PROPIN	proprietary information
RMF	Risk Management Framework
SAR	Selected Acquisition Report
SETA	Systems Engineering and Technical Assistance
SIPRNet	Secret Internet Protocol Router Network
STIG	Security Technical Implementation Guide
TSA	Trade Secrets Act
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Undersecretary of Defense for Intelligence
WHS/EITSD	Washington Headquarters Services, Enterprise Information Technology Services Directorate

Introduction

Acquisition data provide important insights for defense policymakers.¹ They are central to assessing program performance and to program management. Their nature, however, makes them inherently sensitive—and compels the government to balance the need to protect private firms’ interests with the requirements of those who provide analytical and managerial capabilities to the government.

Several government-wide policies mandate that agencies protect sensitive data. The Federal Information Security Management Act (FISMA)² tasks each agency with developing, documenting, and implementing an information security strategy.³ The Open Data Policy requires agencies to “strengthen measures to ensure that privacy and confidentiality are fully protected and that data are properly secure.”⁴ It also requires agencies to “incorporate privacy analyses into each stage of the information’s life cycle.”⁵

In addition to security policy that protects and properly secures critical acquisition data, Executive Order 13556, “Controlled Unclassified Information [CUI],”⁶ established the CUI program to help simplify the handling of unclassified information:

[The CUI program] is a system that standardizes and simplifies the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies. The program emphasizes the openness and uniformity of government-wide prac-

¹ 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 \$1.6 trillion portfolio of major weapon programs by the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD(AT&L)).

² U.S. Congress, 107th Cong., E-Government Act of 2002, Washington, D.C., H.R. 2458, Public Law 107–347, December 17, 2002. 44 U.S.C. 3541, et seq.

³ The individual data systems (e.g., Defense Acquisition Management Information Retrieval [DAMIR]) are required to develop and promulgate a security classification guide to address data aggregation or compilation issues in accordance with U.S. Department of Defense Manual (DoDM) 5205.02-M, *DoD Operations Security (OPSEC) Program Manual*, Washington, D.C., November 3, 2008; and DoDM 5200.01, Vol. 1, *DoD Information Security Program: Overview, Classification, and Declassification*, Washington, D.C., February 24, 2012; however, this report does not provide guidelines on how the data system program manager can determine whether data aggregation or compilation issues exist. Aggregation and compilation of controlled unclassified information (CUI) will be examined as part of a follow-on study.

⁴ Executive Office of the President, Office of Management and Budget, *Open Data Policy-Managing Information as an Asset*, Washington, D.C., May 9, 2013, p. 9.

⁵ Executive Office of the President, Office of Management and Budget, 2013, p. 9.

⁶ Executive Order 13556, *Controlled Unclassified Information*, Washington, D.C.: The White House, November 4, 2010.

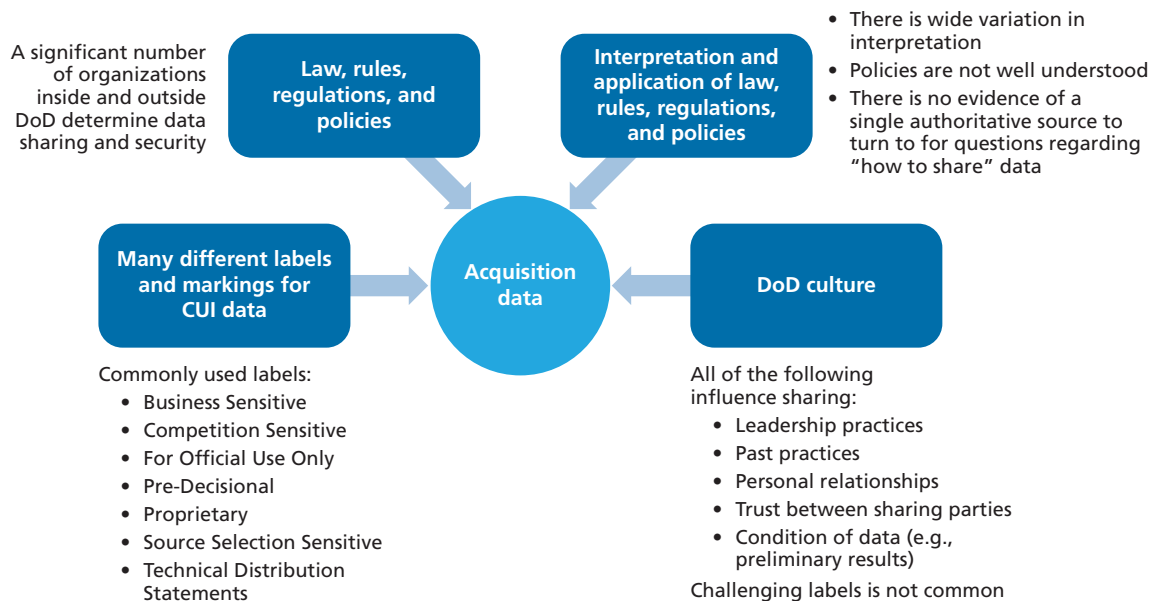
tices. Its purpose is to address the current inefficient and confusing patchwork that leads to inconsistent marking and safeguarding as well as restrictive dissemination policies, which are often hidden from public view.

The President has designated the National Archives and Records Administration (NARA) as the CUI Executive Agent (EA). In this role, NARA has the authority and responsibility to oversee and manage the implementation of the CUI program and will issue policy directives and publish reports on the status of agency implementation.⁷

In our earlier work on managing and sharing acquisition data,⁸ we found a complex set of rules and practices governing CUI labels and security policies for acquisition data, as illustrated in Figure 1.1.

Acquisition leadership within the U.S. Department of Defense (DoD) and supporting government and nongovernment analysts must have maximum visibility of these acquisition data in order to make critical decisions regarding major programs. The Deputy Director, Acquisition Resources and Analysis (ARA), Enterprise Information (EI), within OUSD(AT&L) is leading efforts to manage these data as part of its core mission to improve acquisition data collection and management.

Figure 1.1
Influences on Access to Acquisition Data



SOURCE: RAND analysis based on Riposo et al., 2015.

RAND RR1476-1.1

⁷ Controlled Unclassified Information Office, *What Is CUI? Answers to the Most Frequently Asked Questions*, Washington, D.C.: U.S. National Archives and Records Administration, 2011.

⁸ Jessie Riposo, Megan McKernan, Jeffrey A. Drezner, Geoffrey McGovern, Daniel Tremblay, Jason Kumar, and Jerry M. Sollinger, *Issues with Access to Acquisition Data and Information in the Department of Defense: Policy and Practice*, Santa Monica, Calif.: RAND Corporation, RR-880-OSD, 2015.

RAND has been supporting these efforts. Earlier research explored the general difficulties in getting access to acquisition data.⁹ In this report, the authors explore in greater depth issues regarding proprietary information (PROPIN), labeling and marking of CUI, and the workings of security policies in two information systems.

Approach

Our work for this phase of research on managing and handling acquisition data within 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 OUSD(AT&L). We executed our work through three main tasks.

Task 1: 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 government employees, contractor originators who provide 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. We developed a range of options for improving direct access for nongovernment employees to proprietary data and documented the options that OUSD(AT&L) is pursuing to improve sharing. We characterized the options and their advantages and disadvantages and assessed implementation strategies for them.

Task 2: Characterize commonly used data markings that support acquisition decisionmaking 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) decisionmaking and oversight is intimately connected to acquisition data access, research, and analysis. Whether these data are available for timely, actionable decisionmaking 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.

Task 3: 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 OUSD(AT&L)—the Acquisition Information Repository (AIR) and 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 policies and identified how particular policies affect OUSD(AT&L)'s ability to provide access to acquisition data and manage acquisition data.

⁹ Riposo et al., 2015.

Organization of This Report

The remaining chapters in this report include Chapter Two on proprietary information, Chapter Three on the origins of commonly used acquisition labels, and Chapter Four on security policy as it affects the management of two information systems in OUSD(AT&L). Chapter Five shares our conclusions and options for mitigating the problems identified in the chapters.

Our recommendations are designed to help the government regain its ability to conduct oversight and management that has been lost due to workforce policies that have greatly diminished DoD's organic analytic capabilities. In other words, a diminishing government workforce has caused an ever-greater reliance on support contractors. We note that the RAND Corporation operates three FFRDCs: RAND Project AIR FORCE, RAND Arroyo Center, and the RAND National Defense Research Institute. Because RAND's FFRDCs access and analyze CUI as part of their research, changes in data access for FFRDCs would also apply to those housed at RAND. We note this to make the reader aware of the possibility of conflict of interest. However, our research is intended to advance the broader discussion of how DoD can improve oversight of its acquisition programs, in which capacity it draws on the analytic capabilities of a range of organizations.

Proprietary Information: Clarifying and Creating Confusion

In our earlier work,¹ we found that sharing and handling PROPIN within DoD is challenging because companies submitting information to the government want to keep certain information confidential for legitimate business reasons. DoD use of contract support, however, raises concerns about the proper handling and protection of this sensitive information. Some contractors² may have a conflict of interest if they are granted access to sensitive information from other companies.

Moreover, while government employees are aware that nongovernment employees conducting analysis shall not have access to proprietary data without permissions from the contractor originator who provided these data, they may not be aware that all government employees may view these data for official purposes without additional permissions from the contractor.³ Despite some policies that attempt to define PROPIN and handling restrictions, significant confusion exists within DoD about what information is truly proprietary (and therefore restricted), who can have access to the information, and how to grant access when needed.

Our earlier work described the scenarios in which DoD relies on nongovernment personnel to receive, retransmit, and analyze potential PROPIN. We concluded:

[T]he PROPIN environment has created a situation whereby the government has initially restricted contractor access to PROPIN data, then subsequently begun a patchwork process of granting access in limited circumstances. But the patchwork process is incomplete.⁴

This “patchwork” inhibits DoD’s ability to use contractor support, restricts the flow of information, and limits analyses of available data that could drive positive changes. The PROPIN situation is further complicated by apparent shifts over time in how some contractors are categorized. We attempted to identify possible policy options for DoD to consider that might help ease the flow of information to those with the requisite need, but we found that current DoD legal interpretations of the Trade Secrets Act (TSA) are preventing contractor access to PROPIN.

¹ Riposo et al., 2015.

² This applies only to non-FFRDCs because there are restrictions on FFRDCs that require no conflict of interest.

³ The data provided to the government under contract with a company are initially marked by the contractor. If the contractor feels that the information is proprietary, the contractor marks it as such. In order for the government to share non-technical proprietary information with support contractors, each individual recipient of the data must sign a nondisclosure agreement (NDA) with the company that provided the data to the government.

⁴ Riposo et al., 2015, p. 29.

What Is Truly Proprietary Information?

This section attempts to shed light on the meaning of the term “PROPIN” as used by DoD and to identify sources of confusion and conflict in the understanding of the term. As described below, there are several different sources of law and policy that attempt to define and govern PROPIN. Some of these are clear, but others are less specific. Some seem to suggest limitations on the use of the PROPIN label, while others seem to open the door to indiscriminate labeling of privately owned data by prime contractors (originators of that information) as proprietary, thus restricting its use for acquisition purposes.

DoD Policy

DoD defines “proprietary” in DoD Instruction (DoDI) 5230.24 as follows:

Information relating to or associated with a company’s products, business, or activities, including, but not limited to, financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and knowledge that have been clearly identified and properly marked by the company as “proprietary information,” trade secrets, or company confidential information. The information must have been developed by the company and not be available to the Government or to the public without restriction from another source.⁵

Companies are responsible for labeling information as proprietary, but there is no requirement to mark the discrete portions of the information that are PROPIN. By contrast, classified information procedures require each paragraph to be labeled with the appropriate level of classification—known as “portion marking.” Because company submissions to DoD simply have a blanket label of “proprietary”—often in the form of a header or footer printed on a document—government personnel have no cues as to what specific information is asserted to be proprietary within a particular document. For example, submissions to the Performance Assessment and Root Cause Analysis (PARCA) office’s Earned Value Management Central Repository (EVM-CR) contain the company’s name and the contract number, neither of which is proprietary. Nevertheless, the entire submission is usually labeled “proprietary” by the company. From interviews with DoD personnel and the professional experiences of RAND staff, the government personnel feel obligated to treat a company’s entire submission as proprietary—making no attempt to parse what is and is not PROPIN—and to restrict nongovernment personnel from accessing the information in its entirety. This is despite the fact that it is ultimately the responsibility of DoD personnel to determine what information should be treated as proprietary for internal handling purposes and for potential disclosures in response to Freedom of Information Act (FOIA) requests. The prevailing indiscriminate treatment of information as proprietary can unnecessarily restrict the flow of information and limit the government’s ability to receive analytic support from nongovernment personnel.

⁵ DoDI 5230.24, 2012, p. 29.

The Trade Secrets Act

In our previous work, we noted the role of the TSA⁶—codified at United States Code (U.S.C.) Title 18, Section 1905⁷—in defining PROPIN and the relevant restrictions. However, the TSA also fails to provide specifics about what is and is not PROPIN, and we could not find any case law defining or clarifying the definition of PROPIN.⁸ This is largely because the TSA is a criminal provision, so relevant cases involve government personnel attempting to personally gain by selling a company’s sensitive information to a competitor. Our work is focused on government personnel making good faith judgments about what is and is not PROPIN and allowing nongovernment personnel proper access accordingly. The absence of a clear definition of PROPIN creates uncertainty (and, thus, fear of prosecution among government personnel) when trying to articulate how the TSA applies to the use of PROPIN for legitimate governmental purposes at DoD.

Freedom of Information Act Exemption 4

Another source of authority that provides guidance regarding the definition of PROPIN is Exemption 4 of the FOIA. This restricts release of “(1) trade secrets and (2) commercial or financial information obtained from a person and privileged or confidential.”⁹ The FOIA does not provide specific definitions for these types of information, but case law and secondary sources interpreting FOIA cases has helped define what is PROPIN. For example, the U.S. Department of Justice (DOJ) FOIA guide on Exemption 4 states:

Finally, it should be noted that the Trade Secrets Act—a broadly worded criminal statute—prohibits the disclosure of much more than simply “trade secret” information and instead prohibits the unauthorized disclosure of all data protected by Exemption 4. . . . Indeed, the Court of Appeals for the District of Columbia Circuit and nearly every court that has considered the issue has found the Trade Secrets Act and Exemption 4 to be “coextensive.” Thus, the D.C. Circuit held that if information falls within the scope of Exemption 4, it also falls within the scope of the Trade Secrets Act. . . .

The practical effect of the Trade Secrets Act is to limit an agency’s ability to make a discretionary release of otherwise exempt material, as a submitter could argue that a proposed release of such information would constitute “a serious abuse of agency discretion” redressable through a reverse FOIA suit. Thus, in the absence of a statute or properly pro-

⁶ Riposo, et al., 2015, p. 24.

⁷ 18 U.S.C. 1905.

⁸ 18 U.S.C. 1839 defines “trade secret” as

(3) all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and

(4) the term “owner”, with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.

⁹ 5 U.S.C. 552(b)(4).

mulgated regulation giving the agency authority to release the information—which would remove the disclosure prohibition of the Trade Secrets Act—a determination by an agency that information falls within Exemption 4 is “tantamount” to a decision that it cannot be released.¹⁰

Since information falling within the scope of FOIA Exemption 4 also falls within the scope of the TSA, we can look to Exemption 4 cases for guidance about what might constitute PROPIN. The courts differentiate between information that must be provided to the government and information that is voluntarily provided to the government. For purposes of this study, we are focused on information required by the government.

In the seminal decision on this issue, the D.C. Court of Appeals created a two-part test—which has been widely adopted in other circuits—to determine whether commercial or financial information is “confidential” and thus protected from disclosure under Exemption 4:

[C]ommercial or financial matter is “confidential” for purposes of the exemption if disclosure of the information is likely to have either of the following effects: (1) to impair the Government’s ability to obtain necessary information in the future; or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained.¹¹

Because companies are required to submit financial and other nontechnical information to satisfy the terms of their contracts with DoD, it is unlikely that disclosure would impair the government’s ability to obtain it in the future. We are therefore most interested in the second part of the court’s test regarding whether disclosure would “cause substantial harm to the competitive position” of the company. The DOJ FOIA guide makes clear that there is no blanket rule for what constitutes competitive harm and that government agencies need to “carefully conduct a thorough competitive harm analysis on a case-by-case basis.”¹² The DOJ FOIA guide summarizes several court decisions that held that various types of information were “confidential” under Exemption 4:

Numerous types of competitive injury have been identified by the courts as properly cognizable under the competitive harm prong, including the harms generally caused by disclosure of:

- (1) detailed financial information such as a company’s assets, liabilities, and net worth;
- (2) a company’s actual costs, break-even calculations, profits and profit rates;
- (3) data describing a company’s workforce that would reveal labor costs, profit margins, and competitive vulnerability;
- (4) a company’s selling prices, purchase activity, and freight charges;

¹⁰ U.S. Department of Justice, *Department of Justice Guide to the Freedom of Information Act*, Washington, D.C., 2009, p. 354.

¹¹ *Nat’l Parks & Conservation Ass’n v. Morton*, 498 F.2d 765, 770 (D.C. Cir. 1974).

¹² U.S. Department of Justice, 2009, p. 339.

- (5) shipper and importer names, type and quantity of freight hauled, routing systems, cost of raw materials, and information constituting the “bread and butter” of a manufacturing company;
- (6) market share, type of product, and volume of sales;
- (7) “currently unannounced and future products, proprietary technical information, pricing strategy, and subcontractor information,” and similar data; and
- (8) raw research data used to support a pharmaceutical drug’s safety and effectiveness, information regarding an unapproved application to market the drug in a different manner, and sales and distribution data of a drug manufacturer.¹³

The DOJ FOIA guide also includes the following examples of courts ultimately not finding that information was “confidential” under Exemption 4 (and was thus not PROPIN):

- “[P]rotection under the competitive harm prong has been denied when the prospect of injury is remote—for example, when a government contract is not awarded competitively—or when the requested information is too general in nature.”¹⁴
- “There are many well-reasoned decisions upholding agency determinations to disclose unit prices in the absence of convincing evidence of competitive harm.”¹⁵
- “[T]here are three other cases which contain a thorough analysis of the possible effects of disclosure of unit prices—including two appellate decisions—and in all three of these cases the courts likewise denied Exemption 4 protection, finding that disclosure of the prices would not directly reveal confidential proprietary information, such as a company’s overhead, profit rates, or multiplier, and that the possibility of competitive harm was thus too speculative.”¹⁶

The public interest is also a part of decisions about what information companies can restrict. As declared in two cases:

- “[W]e must balance the strong public interest in favor of disclosure against the right of private businesses to protect sensitive information. . . . Based on the record in this case, we believe that FOIA’s strong presumption in favor of disclosure trumps the contractors’ right to privacy. Those seeking to prevent disclosure of certain information under FOIA have the burden of proving that the information is confidential.”¹⁷
- “[T]he disclosure contemplated as the chief virtue of FOIA is not merely to make accessible just any information in the government’s possession, but in particular to expose information which would ‘open agency action to the light of public scrutiny.’ . . . ‘Official information that sheds light on an agency’s performance of its statutory duties falls squarely within that statutory purpose.’ . . . In perhaps no sphere of governmental activity would that purpose appear to be more important than in the

¹³ U.S. Department of Justice, 2009, p. 324.

¹⁴ U.S. Department of Justice, 2009, p. 328.

¹⁵ U.S. Department of Justice, 2009, p. 339.

¹⁶ U.S. Department of Justice, 2009, p. 342.

¹⁷ *GC Micro Corp. v. Def. Logistics Agency*, 33 F.3d 1109 (9th Cir. 1994) at 1115.

matter of government contracting. The public, including competitors who lost the business to the winning bidder, is entitled to know just how and why a government agency decided to spend public funds as it did; to be assured that the competition was fair; and, indeed, even to learn how to be more effective competitors in the future.”¹⁸

Ultimately, based on the researchers’ understanding of current practice, the company submitting nontechnical data to the government is responsible for asserting that certain portions are proprietary, but the government recipient is responsible for initially determining whether to accept that assertion and for maintaining the “proprietary” label. For public disclosure, the government would have to inform the company submitter of a determination that all or part of the submission is not proprietary, giving the company submitter a chance to file a lawsuit to stop disclosure—referred to as a “reverse FOIA” case. However, the procedure for allowing internal support contractors access to the company submitter’s information is less clear. If the responsible government official determines that the information is not proprietary, the government official may not be obliged to inform the company submitter of the determination. To remain consistent, DoD officials may find it advisable to inform companies that submit data of an initial determination that all or part of the submissions will not be treated as proprietary, along with the justification for that determination.

If the government official wants to publicly disclose the information in response to a FOIA request, then the government official 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.

Who Can Access PROPIN?

There is confusion among DoD personnel about who can access PROPIN. PROPIN that is not specifically restricted (e.g., source selection information) can be treated like all other CUI, meaning that all government employees are authorized to access the information for official purposes. This access is enabled by virtue of the fact that the government has obtained the information under a lawful requirement and is based on longstanding interpretations of the TSA by DOJ.¹⁹ Here we explore which types of PROPIN can be shared with nongovernment entities.

Technical Data

Federal law permits DoD to grant access to “technical data”²⁰ by “covered government support contractors” in accordance with 10 U.S.C. 2320. This allows the Secretary of Defense to grant

a covered Government support contractor access to and use of any technical data delivered under a contract for the sole purpose of furnishing independent and impartial advice or

¹⁸ *Martin Marietta Corp. v. Dalton*, 974 F. Supp. 37 (D.D.C. 1997) at 40.

¹⁹ See, e.g., William Michael Treanor, “Applicability of Trade Secrets Act to Intra-Governmental Exchange of Regulatory Information,” memorandum, Office of Legal Counsel, U.S. Department of Justice, April 5, 1999.

²⁰ As defined by 22 CFR 120.10.

technical assistance directly to the Government in support of the Government's management and oversight of the program or effort to which such technical data relates.²¹

Among other things, the "covered government support contractor" must meet all of the following requirements:

- The contractor must not be "affiliated with the prime contractor."²²
- The contractor must "enter into a non-disclosure agreement with the contractor to whom the rights to the technical data belong."²³
- The contractor must not use the disclosed technical data to "compete against the third party for Government or non-Government contracts."²⁴

The NDA requirement in 10 U.S.C. 2320 has been implemented through a contract provision contained in the Defense Federal Acquisition Regulations Supplement (DFARS). This states:

(iv) The Contractor acknowledges that—

(A) Limited rights data are authorized to be released or disclosed to covered Government support contractors;

(B) The Contractor will be notified of such release or disclosure;

(C) The Contractor (or the party asserting restrictions as identified in the limited rights legend) may require each such covered Government support contractor to enter into a non-disclosure agreement directly with the Contractor (or the party asserting restrictions) regarding the covered Government support contractor's use of such data, or alternatively, that the Contractor (or party asserting restrictions) may waive in writing the requirement for a non-disclosure agreement[.]²⁵

In other words, the contractor submitting the technical data to DoD can choose to sign an NDA with each covered government contractor or waive the NDA requirement, but ultimately the covered government support contractor must be granted access to technical data by the prime contractor, even if it is PROPIN.

Nontechnical Data

The much greater challenge for DoD has been the treatment of nontechnical data that may be PROPIN. The only statute that directly addresses nongovernment entities accessing nontechnical data is 10 U.S.C. 129d. This allows "litigation support contractors" access to "commer-

²¹ 10 U.S.C. 2320(c)(2).

²² 10 U.S.C. 2320(f).

²³ 10 U.S.C. 2320(f).

²⁴ 10 U.S.C. 2320(f).

²⁵ 48 CFR 252.227-7013, Rights in technical data—Noncommercial items. The contract can also contain another provision that limits disclosure. See 48 CFR 252.227-7025.

cial, financial, or proprietary information, technical data, or other privileged information”²⁶ without an NDA. The purpose of this law is to ensure that the government can use contractors to augment staff during litigation.

However, the vast majority of nongovernment personnel and nontechnical data do not fall into the litigation support category, and DoD personnel have grappled with how to address these circumstances in the absence of clear guidance.

Determining How to Grant Access to PROPIN

DoD faces perhaps its most significant PROPIN challenge in determining how to grant access to PROPIN. Government personnel have the discretion to provide nongovernment entities access to nonpublic information (e.g., to nongovernment entities who need the information to carry out their government contract). For technical data, laws and policies provide sufficient guidance for creating procedures to allow nongovernment personnel to access this type of data. Unfortunately, there is no specific guidance either for nontechnical PROPIN or for the different categories of nongovernment personnel.

Distinctions Among Nongovernment Entities

The primary distinction between nongovernment personnel for purposes of data access and analytic support is between contractors, generally, and for the special case of FFRDCs.²⁷ Multiple federal statutes reference permissible activities associated with FFRDCs, making clear that they are different from other contractors. For example, 10 U.S.C. 2367, “Use of Federally Funded Research and Development Centers,” makes clear that DoD must have a “sponsoring agreement” that specifies “the purpose, mission, and general scope of effort of such center.”²⁸ DoD can use noncompetitive procedures to assign work to FFRDCs²⁹ under 10 U.S.C. 2304, “Contracts: Competition Requirements.” DoD must also report to Congress the “man-years of effort expended at each” FFRDC after the end of each fiscal year.³⁰ Further, FFRDCs are considered “other organizations”³¹ under federal personnel law and, as such, are permitted to conduct work through Intergovernmental Personnel Act (IPA) assignments, during which FFRDC staff are treated as special government employees, while remaining employed by their home organizations.

The Federal Council for Science and Technology created criteria for FFRDCs in a 1967 memorandum.³² The Office of Federal Procurement Policy added provisions to the Federal

²⁶ 10 U.S.C. 129d(b).

²⁷ We remind the reader that the division of the RAND Corporation that conducted this work is an FFRDC.

²⁸ 10 U.S.C. 2367(a).

²⁹ 10 U.S.C. 2304(c)(3).

³⁰ 10 U.S.C. 2367(d).

³¹ 5 U.S.C. 3371(4)(D).

³² National Science Foundation, “Master Government List of Federally Funded R&D Centers: General Guidelines,” June 2015b, citing “Hornig DF. 1967. Memorandum to members of Federal Council for Science and Technology. Subject: Federally funded research and development centers. Unpublished memorandum from the Federal Council for Science and Technology, Executive Office of the President, Washington DC, 1 November.”

Acquisition Regulations (FAR) regarding FFRDCs in 1984.³³ The National Science Foundation maintains the “Master Government List” of FFRDCs.³⁴ The FAR provisions³⁵ distinguish FFRDCs from contractors in several ways, including the following:

- “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.”³⁶ (Emphasis added.)
- The FFRDC sponsoring agreement must include “[a] *prohibition against the FFRDC competing with any non-FFRDC concern* in response to a Federal agency request for proposal for other than the operation of an FFRDC.”³⁷ (Emphasis added.)
- The FFRDC sponsor must ensure that “[t]he FFRDC is operated, managed, or administered by an autonomous organization or as an identifiably separate operating unit of a parent organization, and is required to operate *in the public interest, free from organizational conflict of interest*, and to disclose its affairs (as an FFRDC) to the primary sponsor.”³⁸ (Emphasis added.)

The second point above is particularly interesting from the standpoint of FFRDC access to data that might be sensitive based on competition for federal contracts. FFRDCs are forbidden from competing for DoD work. The primary underlying policy reason for protection of competition-sensitive data is to protect the data owner from being disadvantaged in a future competition, which could happen if a competitor got access to that data. However, the potential for competitive harm does not exist with respect to FFRDCs because FFRDCs are barred from competing for contracts.

Within DoD, formal and informal policies further highlight how FFRDCs are different than other government contractors. For example, a 2011 memorandum from the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), noted the “special relationship” DoD has with FFRDCs and the FFRDCs’ “freedom from organizational conflict of interest.”³⁹ The Army regulation for the RAND Arroyo Center FFRDC states, “Following sponsor or COR [Contracting Officer’s Representative] authorization [of a project], Army activities will release required classified, privileged, proprietary, or sensitive material directly to the FFRDC.”⁴⁰ Evidence demonstrates that under existing laws, regulations, and policies, DoD treats FFRDCs as distinct from other contractors.

³³ National Science Foundation, 2015b.

³⁴ National Science Foundation, “Master Government List of Federally Funded R&D Centers,” June 2015a.

³⁵ Currently part of the Code of Federal Regulations in 48 CFR 35.017, et seq.

³⁶ 48 CFR 35.017(a)(2).

³⁷ 48 CFR 35.017-1(c)(4).

³⁸ 48 CFR 35.017-2(h).

³⁹ Ashton B. Carter, “Federally Funded Research and Development Center (FFRDC) Management Plan and Associated ‘How-to-Guides,’” memorandum, Washington, D.C.: Acquisition, Technology and Logistics, Department of Defense, May 2, 2011.

⁴⁰ U.S. Army, “Management: RAND Arroyo Center,” Army Regulation 5-21, Washington, D.C.: Headquarters Department of the Army, May 25, 2015, p. 2.

Apparent Shift in Data Access Procedures for Nontechnical Data

Despite federal regulations allowing FFRDCs access to PROPIN, the DoD Office of General Counsel (OGC) appears to have shifted its interpretation of how FFRDCs should be treated in recent years. Before 2012, several FFRDC staff members had been granted unrestricted access to the Defense Acquisition Cost Information Management System (DACIMS) and the EVM-CR, which contain data on costs associated with contracts for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAISs), some of which may be PROPIN.⁴¹ However, this access was terminated in May 2014. According to interviews with DoD personnel, this change was based on oral guidance from the DoD OGC. These personnel indicated that DoD OGC staff members believe that FFRDCs should be treated the same as other contractors and, therefore, could not be allowed access to PROPIN. Further clarifications requested by Office of the Secretary of Defense (OSD) personnel to DoD OGC resulted in DoD OGC oral and draft written guidance stating that each FFRDC staff member must have a one-to-one NDA with each contractor that has information in DACIMS and EVM-CR. The unpublished DoD OGC guidance also indicated an interpretation of the TSA that effectively renders inoperative the FAR provision on FFRDC data access, 48 CFR 35.017(a)(2).

Over the course of this research, we were unable to locate a signed DoD OGC legal opinion stating this interpretation. The only DoD OGC legal opinion on this topic that we could obtain is dated February 1999⁴² and does not discuss whether NDAs are required for FFRDCs (this memo is provided in the appendix). The 1999 opinion simply approves an existing procedure involving NDAs for contractors to access cost data and the voluntary application of that procedure to FFRDCs. The 1999 opinion specifically quotes “FAR 35.017”—what is officially codified as 48 CFR 35.017(a)(2)—and states that it is “reasonable” to allow FFRDCs access to certain information beyond what contractors can be allowed.⁴³

Regardless of what previous DoD OGC opinions may have stated, the change from long-standing practice of FFRDC access to DACIMS and EVM-CR (without NDAs) was prompted by verbal rather than written or documented guidance from DoD OGC personnel to OSD personnel. The effect of this shift to an NDA requirement is covered in our earlier work.⁴⁴ The result has been that data managers have created a number of ad hoc processes for monitoring the large number of NDAs and appropriate permissions required for nongovernment personnel to access the nontechnical proprietary data in these information systems. These processes are not formalized and lack dedicated staff and resources to ensure that NDAs are signed in a timely fashion.

Based on our understanding of current DoD OGC guidance and practices within parts of OSD, all nongovernment personnel working for DoD are required to have one-to-one NDAs before accessing any nontechnical PROPIN. In other words, each employee of a support contractor or FFRDC who needs to access information that is potentially PROPIN must have a signed NDA with each company originator that supplies information into a database.

⁴¹ Riposo et al., 2015, p. 19.

⁴² Karen Grosso, “Memorandum for the Director, Contractor Cost Data Report Project Office,” memorandum, Washington, D.C.: Office of the Deputy General Counsel (Acquisition and Logistics), Department of Defense, February 1, 1999.

⁴³ Grosso, 1999.

⁴⁴ See, e.g., Riposo et al., 2015, p. 14.

However, we are also aware that this practice has not been adopted uniformly across DoD, or even in all of OSD.

How DoD Is Addressing PROPIN

We initially identified several policy options that could potentially streamline nongovernment personnel access to PROPIN and improve efficiency and effectiveness of external support. For example, we suggested to DoD personnel that the FAR FFRDC provisions could be used to exempt FFRDCs from the NDA requirement, or that they could be covered by a blanket NDA with DoD.

For other contractors, we also recommended that DoD consider the following actions:

- creating a DFARS provision that would cover nontechnical data,⁴⁵ 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.

Changes to regulation and legislation both come with drawbacks. DoD can propose changes to the DFARS without congressional action and presidential approval, but changing the DFARS might not adequately include previous PROPIN designations because a new clause would only affect contractors that have active DoD contracts. Changing the law would require congressional action and presidential approval, take at least two years, and may result in unwanted changes.

At the time of this study, DoD personnel indicated that they intended to propose changing the law only to clarify and reduce the requirements for FFRDCs (and in effect, returning to the practices that had been in effect for many years). This change, if successful, would not take effect any earlier than October 1, 2016.⁴⁶ It would also address PROPIN access for only the small percentage of persons who support DoD that are housed in FFRDCs and would leave in place the existing patchwork approach and lack of clarity for other support contractors about who is required to do what to access PROPIN. DoD will continue to encounter limits in support from nongovernment personnel until the matter is resolved. Perhaps just as important, DoD personnel will continue to work without clarity about uniform procedures and will likely continue to treat the entire contents of all contractor submissions labeled “proprietary” as PROPIN without attempting to identify the discrete pieces of information or data that actually merit protection as PROPIN.

⁴⁵ As noted above, 10 U.S.C. 2320 specifically addresses technical data, so we are only discussing nontechnical data.

⁴⁶ Legislative proposals such as the one summarized here would be included in the annual National Defense Authorization Act (NDAA). This specific proposal is intended to be part of the Fiscal Year 2017 NDAA, which would not take effect any earlier than October 1, 2016.

Origins and Meaning of Commonly Used Controlled Unclassified Information Labels on Acquisition Data

In the previous chapter, we provided a detailed analysis of the treatment of PROPIN—a special class of CUI that relates to information and data developed by a private entity but shared with the government and which can potentially be further shared with nongovernment entities. The PROPIN protections arise from numerous and potentially conflicting sources of law and policy. The effect of labeling information as proprietary is a system of special handling procedures that govern who has access to the data, at what times, and for what purposes. Yet PROPIN is merely one of a host of labels that are put on data. Classified information, for example, is commonly recognized as having a clear and definitive system for information labeling, access, and control. Classified information seldom raises similar concerns about labeling and access, likely because of the clear policy, dedicated office with jurisdiction over classified information security, and the attention to the special care and handling that classified information requires.

The same degree of care, handling, and attention given to classified information cannot be said of the system governing CUI. The broader category of CUI certainly has a system of markings to demonstrate that the information is sensitive. Yet these labels are not as clear, well managed, or well understood as the system surrounding classified information.¹

In this chapter, we look at CUI labels that are commonly used by DoD as part of the acquisition process. We identify commonly used labels, summarize their basis in law and policy, and determine whether the policy prescriptions they provide for data labeling and access are clear, consistent, and in accord with the OUSD(AT&L) goals. Properly identifying and managing potentially sensitive information can help to facilitate analysis and ultimately improve the functioning of DoD.

OUSD(AT&L) decisionmaking and oversight are intimately connected to access to data, as well as to research and analysis that are grounded in acquisition data. Whether these data are available for timely, actionable decisionmaking partially depends on the type of data, the data control system, and the ability of data users to properly identify, label, and, if needed, challenge improper markings on data.

¹ The study team did not evaluate whether adopting a system similar to the classified labeling procedures would help to fix some of the challenges identified in labeling CUI.

Guiding Questions and Choice of Labels

In our earlier work,² we found that unclassified acquisition data and related information take several forms (e.g., hard copies, digital repositories, structured data, and unstructured data). Many of these are exchanged between government and nongovernment entities throughout the acquisition process. The data and derivative analyses are governed by a system of labels and markings, rules, regulations, and policies. Some of these are well-established policies that reflect current understanding of the law and regulatory environment for data protection and data sharing. Others are outdated, legacy markings and practices. The labeling of CUI is complicated by the fact that no single, consolidated policy lists and explains the various labels (although there are a few core references in DoD policy, such as DoD Manual 5200.01, Vol. 4, *DoD Information Security Program: Controlled Unclassified Information [CUI]*).

Furthermore, the data marking and labeling process is infused with individual judgment and interpretation. The rules in place for data labeling are not always clear cut and are rarely subjected to an oversight regime that would assist in the development of standardization. The previous chapter demonstrated the difficulty in applying the PROPIN label consistently across numerous department and industry partners. The subjectivity and diversity in approaches to data labeling are further magnified and complicated by the sheer number of DoD offices that have a role in the creation of policy for data handling and management, as well as the number of individuals actually making the determination about what labels to place on the data they use or produce.

Ultimately, there is no single authoritative source to answer questions regarding “how to share” data. We sought to clarify the current landscape of the most commonly used data labels, their roots in law and policy, and the ways they operate within the DoD controlled unclassified data labeling system. To guide our study of the labeling regime for CUI, we identified the following key questions:

- What labels are most commonly placed on acquisition information or data?
- What is the rationale (i.e., justification or reason for protecting the data) for use of the label?
- What is the legal, regulatory, or policy basis for using the label?
- Does the label’s basis or other guidance adequately define what type of information should be labeled?
- Is the method to protect the data defined, along with who is responsible for controlling access?
- Which nongovernment entities (if any) are allowed access to the data?

We also identified the DoD policy owners. “Policy owners” refers to the organizations that authorized the policies that created the basis for each of the labels identified below.

With senior staff from OUSD(AT&L)’s Office of Acquisition Resources and Analysis, we identified seven data labels that are commonly used as an indicator that information requires some type of special handling or restriction on access:

- Business Sensitive

² Riposo et al., 2015.

- Competition Sensitive
- For Official Use Only
- Pre-Decisional
- Proprietary
- Source Selection Sensitive
- Technical Distribution Statements.

We sought to understand what each label means, how it was applied, and its basis—that is, the official, legal, regulatory, or policy foundation for such a label. A label’s basis may be in

- **Case law.** Court cases can provide authoritative interpretations of laws and, in some cases, are the sources of data labels. If a Supreme Court case defines a term, that definition supersedes all other interpretations of the term.
- **Statutory law.** Terms in law (statute, generally the U.S.C.) are the highest authority for a label in the absence of a court decision.
- **Regulation.** Terms in regulations (e.g., FAR provisions, other provisions of the Code of Federal Regulations [CFR]) have the force of law, subject to any limits in statutory language or through court decisions.
- **Policy.** Policy documents (e.g., DoD Directives [DoDDs], DoDIs) can be a basis as long as they do not contradict regulation, law, or court cases.

We list the sources above hierarchically; any meaning or authorization for data labels at a lower level must be consistent with any superior source of authority if that authority has provided any sort of guidance. A policy document, such as a DoD Instruction (DoDI), must be fully compliant with any applicable law on data access contained in law and regulation; such law or regulation must also be consistent with applicable case law.

Overview of Commonly Used Acquisition Data Labels

In reviewing the data labels, we focus on CUI. As discussed in our earlier work,³ unclassified data are subject to a variety of controls and are being used in ways that are not fully understood by DoD staff. Here we document how some labels are used, their origins, and whether they are grounded in court cases, statute, regulation, policy, or customary use independent of any official source of authorization.

Table 3.1 summarizes the details we reviewed for the seven types of data labels.

The column headings in Table 3.1 correspond to the questions we set out to answer in our study.

Label Placed on Information or Data refers to the banner language that is commonly placed on the data, regardless of whether the label language is grounded in law or policy.

DoD Policy Owner shows which office within DoD has signed the policy that creates or otherwise substantially affects the terms of use for the data label. This identifies who has the responsibility for the data label if there are revisions, challenges, or other feedback relating to the use of the label in practice.

³ Riposo et al., 2015.

Table 3.1
Common Data Labels, Authorization Basis, and Access Details

Label Placed on Information or Data	DoD Policy Owner	Basis	Defined?	Clear Handling Procedures?	Is Nongovernment Access Allowed?
Business Sensitive	ASD(NII)/DoD CIO	DoDI 8520.03	Yes	No	Unclear
Competition Sensitive	Undefined	Sample NDA created by OUSD(AT&L) office	Yes	Yes	FFRDC; contractor access possible
For Official Use Only (FOUO)	USD(I)	Department of Defense Manual (DoDM) 5200.01, Vol. 4	Yes, as exemption to FOIA	Yes	FFRDC; contractor access possible
Pre-Decisional	Undefined	FOIA court cases	Yes	No	Unclear
Proprietary Information (PROPIN)	Undefined	FOIA court cases, law, regulation, policy	Yes, for technical data; No, for nontechnical data	Yes, for technical data; No, for nontechnical data	FFRDC; contractor access possible w/ NDA for tech data; unclear for nontechnical data
Source Selection Sensitive	USD(AT&L)	41 U.S.C. 2102, FAR 2.101, DoD policies	Yes	Yes, "Source Selection Procedures," 2011	FFRDC; contractor access possible
Technical Distribution Statements	USD(AT&L); USD(I)	DoDI 5230.24; DoDM 5200.01, Vol. 4	N/A	N/A	FFRDC; contractor access possible

SOURCE: RAND analysis.

NOTES: ASD(NII) = Assistant Secretary of Defense (Networks and Information Integration); CIO = chief information officer; USD(I) = Undersecretary of Defense for Intelligence.

Basis refers to the source of authority for the label—namely, whether the label is required by case law, statutory law, regulatory guidance, or policy. In the absence of any of these, we noted an available source or example that could be located.

Defined? refers to whether the label is associated with a clear definition for the type of data to which it applies. Definitions may be found in any of the authoritative bases (except for customary use). We indicate whether the types of data to which a label might apply are defined and highlight whether there are certain classes of data (e.g., technical data) that limit the application of the label.

Clear Handling Procedures? indicates whether the label and its associated data are accompanied by a specific program for control and handling. It is possible for a data label to be defined but not accompanied in the same document by a corresponding program of handling and access. Likewise, a data access and handling program could specify clear protections for the data but rely on a definition in policy contained elsewhere.

Is Nongovernment Access Allowed? indicates whether the data can be shared with nonfederal employees, such as IT contractors, SETA support, and FFRDC staff. Some types of data may be shared only with certain classes of nongovernment entities.

Summary of Specific Labels

Business Sensitive: Appears in DoDI 8520.03 (*Identity Authentication for Information Systems*). Access restrictions are not understood because the label is undefined and not part of official labeling policy.

The first label in Table 3.1, “Business Sensitive,” is not based explicitly in statute for DoD purposes (although it does appear in federal law under Title 6, Domestic Security, related to supply chain security cooperation⁴). The “Business Sensitive” label appears in official DoD policy for computer-system identity authentication. DoDI 8520.03, *Identity Authentication for Information Systems*—signed by the CIO—uses the term “Business Sensitive” as a category of information provided by commercial or foreign entities “under the condition that it not be released to other parties.” Implicated in this statement is a set of handling procedures, but DoDI 8520.03 contains no such plan of handling, access, or control for Business Sensitive data.

It is unclear whether the DoDI or common practice by DoD personnel actually means that the label “Business Sensitive” is a substitute for “Source Selection Sensitive” or “Proprietary Information.” There is reasonable overlap between the DoDI definition of “Business Sensitive” information (as commercial or foreign entities’ information that is not to be released) with other categories. But the terms are not identical. DoDI 8520.03’s reference to foreign entities is wholly new to this class of labels. Similarly, the restriction in the DoDI’s definition of information “not to be released to other parties” provides an even stronger restriction on access than PROPIN (which can be shared with other entities upon the satisfaction of additional requirements such as nondisclosure agreements).

Given the loose definition, apparent overlap with existing labels, lack of clear handling procedures, and apparent total ban on sharing data bearing the label “Business Sensitive,” use of this label by DoD personnel may be ill-advised and inappropriate. Documents labeled “Business Sensitive” should be reviewed to determine whether another label is required, and access should be better managed to meet the needs of DoD and the protections required by the data owners.

Competition Sensitive: No identified sources. Access restrictions are not understood because the label is undefined and not part of official labeling policy.

Among the commonly used labels we identified, “Competition Sensitive” is the one with the weakest claim to legitimacy under current policy. The researchers were not able to find the term in known law or policy, but this label may have been part of previous DoD document marking policy.⁵ The only identified use of “Competition Sensitive” appears in an example NDA created by an OUSD(AT&L) organization (date of creation and exact source unknown) for depot maintenance, where the term “Competition Sensitive” is used to expand the definition of “proprietary information.” Consequently, DoD personnel may still be using the label, possibly incorrectly as a substitute for “Source Selection Sensitive” or “Proprietary Informa-

⁴ 6 U.S.C. 985.

⁵ U.S. law and regulation defines several source selection- and procurement-related terms, but “competition sensitive” is not one of them. See, for example, 41 U.S.C. 2101 (Definitions for the Purpose of Clarifying Restrictions on Disclosures of Procurement Information), 41 U.S.C. 2102 (Prohibitions on Disclosing and Obtaining Procurement Information), and 48 CFR 3.104 (Federal Acquisition Regulation on prohibitions, restrictions, and requirements to ensure procurement integrity).

tion” based on the common practice of predecessors or within an organization generally. Documents labeled “Competition Sensitive” should be reviewed to determine whether another label is required and whether access should be restricted. It seems likely that such information would be labeled more appropriately as “Source Selection Sensitive” (see below).

For Official Use Only (FOUO): Basis in DoD policy (DoD Manual 5200.01, Vol. 4). Using the label is often appropriate, and nonpublic access can be granted to nearly anyone as needed. But the label is often misapplied and misunderstood.

The label “For Official Use Only (FOUO)” is likely one of the most commonly applied CUI labels at DoD. It is also likely one of the most misunderstood and misapplied. Our earlier work found that FOUO labeling was somewhat indiscriminate, with infrequent understanding of what triggered such a label.

The basis for the FOUO label is in DoD Manual 5200.01, Vol. 4. This manual, written by USD(I), provides the overarching framework for DoD information security pertaining to CUI. It describes FOUO as “a dissemination control applied by the Department of Defense to unclassified information when disclosure to the public of that particular record, or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected *by one or more of FOIA Exemptions 2 through 9*” (emphasis added).⁶

The language tying use of the FOUO label to FOIA means that before the FOUO label is applied, the document’s creator must ensure that the material fits one of the FOIA exemption categories. The FOIA exemptions that trigger a FOUO label are (per DoDM 5200.01, Vol. 4)

- Exemption 2. Information that pertains solely to the internal rules and practices of the agency that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission.
- Exemption 3. Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
- Exemption 4. Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government’s ability to obtain like information in the future, or impair the government’s interest in compliance with program effectiveness.
- Exemption 5. Inter- or intra-agency memoranda or letters containing information considered privileged in civil litigation.
- Exemption 6. Information, the release of which would reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
- Exemption 7. Records or information compiled for law enforcement purposes.
- Exemption 8. Certain records of agencies responsible for supervision of financial institutions.
- Exemption 9. Geological and geophysical information (including maps) concerning wells.

⁶ “Exemption 1: Information that is classified to protect national security” is not listed here because we are not discussing classified information.

Those eight exemptions above,⁷ and the situations they describe, are the only times when a FOUO label should be applied to a document. The manual further states that the document's originator bears the responsibility of determining whether the information qualifies for the label (and references DoD 5400.7-4 for examples of the types of information that may qualify for the FOUO label).

Concerning access to FOUO information, the manual clarifies that access is meant only for those persons with "a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose." Furthermore, "final responsibility for determining whether an individual has a valid need for access to information designated as FOUO rests with the individual who has authorized possession, knowledge, or control of the information, not with the prospective recipient." More specifically, the manual clarifies that FOUO information "may be disseminated within the DoD Components, and between officials of DoD Components and DoD contractors, consultants, and grantees to conduct business for the Department of Defense, provided that dissemination is consistent with any further controls imposed by a distribution statement."

Pre-Decisional: Basis in court decisions. Use of the label appears to be appropriate, the information that can be included is relatively well characterized, and access can be granted to nearly anyone, as needed.

The label "Pre-Decisional" appears regularly on DoD documents. Its use is appropriate when the document contains information that is being used in a deliberative process leading toward a decision. The term "pre-decisional" is derived from court decisions associated with FOIA Exemption 5. Exemption 5 allows agencies to withhold "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency."⁸ The exemption is intended to allow the free exchange of ideas in government without concern about those deliberations being scrutinized after a decision is made. Court interpretations of Exemption 5 have created a broadly applicable two-part test to determine whether the document fits within the deliberative process privilege⁹:

1. Was it "pre-decisional?" That is, was the information created to support a later decision?
2. Was it part of the deliberative process to make a decision?¹⁰

While not specifically enshrined in DoD policy, "Pre-Decisional" is a legally supported label that can cue a reader about the applicability of Exemption 5. For example, DoDD 7045.14, *The Planning, Programming, Budgeting, and Execution (PPBE) Process* (January 25, 2013), notes that, "Due to the sensitive nature of pre-decisional PPBE information, data release restrictions shall be applied in accordance with this Directive."

In addition to "Pre-Decisional," documents are sometimes labeled "Deliberative" or simply "Draft" to alert the reader about the applicability of FOIA Exemption 5. According to the DoD Freedom of Information Act Program (DoD Regulation 5400.7-R, dated

⁷ Exemption 1 is not included in this total.

⁸ 5 U.S.C. 552(b)(5).

⁹ If the deliberative process privilege applies, the document is exempt from disclosure under FOIA Exemption 5.

¹⁰ Department of Justice FOIA Manual, p. 368.

September 1998), applying Exemption 5 is “entirely discretionary,” meaning that DoD can choose to release information in response to a FOIA request that falls within this definition. However, the decision to release pre-decisional information must still be made by the official responsible for responding to a FOIA request.

Documents that potentially fall within Exemption 5 as “Pre-Decisional” are also often labeled “For Official Use Only (FOUO).” “Pre-Decisional” is sometimes placed on a document when “Source Selection Sensitive” may be more appropriate.

Use in DoD of “Pre-Decisional” appears to be appropriate, the information that can be included is relatively well characterized, and access can be granted to nearly anyone, as needed. The “Pre-Decisional” label needs to be applied by the document creator, the first government organization receiving a document created outside the government, or the government organization entering information into a government computer system.

Proprietary Information: Basis in statutes and court decisions. Using the label can be appropriate, but significant disagreement exists over what is included and who can have access.

The label “Proprietary Information” (sometimes shortened to “PROPIN” or “Proprietary”) appears on DoD documents to indicate that some of the information may have come from a commercial source—i.e., it was submitted to DoD by contractors—and is potentially sensitive. The term “proprietary information” does appear in federal law, but it does not have a specific definition.

The use and definition of “proprietary information” is primarily derived from legal precedent associated with FOIA Exemption 4. Exemption 4 protects information considered “trade secrets and commercial or financial information obtained from a person and privileged or confidential.” Court decisions related to Exemption 4 have repeatedly used “proprietary information” or a similar term. According to the DoD Freedom of Information Act Program (DoD Regulation 5400.7-R, dated September 1998), when “information qualifies as Exemption 4 information, there is no discretion in its release,” meaning that “proprietary information” must not be disclosed in response to a FOIA request. Within DoD, this is relatively well understood when applied to technical data provided by commercial entities.

Specific to DoD, the following laws make reference to “proprietary”:

- 10 U.S.C. 2320, “Rights in Technical Data,” authorizes DoD and support contractors to review certain “technical data” from commercial entities, some of which may be “proprietary.”
- 10 U.S.C. 2321, “Validation of Proprietary Data Restrictions,” applies to “technical data” from commercial entities.
- 10 U.S.C. 129d, “Disclosure to Litigation Support Contractors,” allows DoD contractors providing support for litigation purposes to review “sensitive information,” which includes “proprietary information.”
- 10 U.S.C. 122a, “Public Availability of Department of Defense Reports Required by Law,” requires DoD reports to Congress to be posted on a public website but excludes reports that contain “proprietary information.”

Additional federal law and policy govern proprietary data. The TSA, 18 U.S.C. 1905, is often referred to by DoD personnel as protecting “proprietary information.” This law does not specifically mention “proprietary information,” but it does reference “confidential infor-

mation,” “trade secrets,” and related terms that courts have interpreted as part of “proprietary information” along with FOIA Exemption 4. The FAR also does not define proprietary information (beyond technical data), even though the term appears repeatedly.

Although there is ample law, policy, and regulation about proprietary information, there is significant confusion and disagreement about which financial and management information provided by companies is considered proprietary—and who can access the information—because the term is not defined in statute or policy. Consequently, there have been changing interpretations of what information nongovernment personnel are permitted to access over time.

Court decisions on FOIA Exemption 4 have limited the definition of proprietary, non-technical information to line item pricing data. If a company claims that information is proprietary, it must be able to demonstrate that it will suffer competitive harm “flowing from the affirmative use of proprietary information by competitors,” not simply make a general claim of potential injury to its competitive position. If a government agency chooses to release information that a company claims is proprietary, the company can challenge the government decision through a “reverse FOIA” lawsuit.

While the definition of what is considered proprietary has some basis in court rulings, restrictions on who can access proprietary information are not defined. For example, the FAR contains a provision that allows FFRDCs “access . . . to Government and supplier data, including sensitive and proprietary data” (48 CFR 35.017). According to FAR Council staff in the Office of Federal Procurement Policy, multiple non-DoD agencies abide by FAR 35.017 and allow FFRDC staff access to proprietary information. DoD OGC, however, currently interprets 18 U.S.C. 1905 to mean that government personnel with access to proprietary information cannot share such data with FFRDC personnel because of the threat of criminal prosecution for disclosure. This interpretation would seem to mean that no nongovernment personnel can access proprietary information at any time, barring a specific agreement between the FFRDC staff and the prime contractor who owns the PROPIN. Nevertheless, DoD OGC attorneys have advised some offices that an acceptable approach with nongovernment personnel is to require an NDA that is specific to the person accessing the data and the company that is the source of the data. In other words, each staff member of an FFRDC or other DoD support contractor must sign as many as 100 NDAs to access a DoD database containing potentially proprietary information from all DoD prime contractors.

At the same time, because “proprietary information” is not fully defined in law or regulation, authority to disclose nontechnical information ultimately resides with the DoD official in charge of the data. Because of inconsistent interpretations of laws and regulations, DoD officials are unable to obtain adequate FFRDC and contractor support and may be unwilling to challenge a company’s assertion about the proprietary nature of information.

From a strict labeling perspective, DoD use of “Proprietary Information” or “PROPIN” appears to be generally appropriate. There is legal, regulatory, and policy use of the term, even though its specific usage is still undefined. DoDM 5200.01, Vol. 2, *DoD Information Security Program: Marking of Classified Information*, specifically directs personnel to use “PROPIN” as a “dissemination control” on unclassified information as needed. However, DoDM 5200.01, Vol. 4, *DoD Information Security Program: Controlled Unclassified Information*, only refers to “proprietary information” under controls for “law enforcement sensitive” information. Official DoD policy for marking documents is inconsistent about proprietary information.

While the use of the PROPIN label has a basis in law, court decisions, regulations, and policy, access privileges for proprietary information are not defined, and there is significant confusion and disparity of interpretation within DoD and across the federal government. Based on the researchers' understanding of current practice, 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 maintain the "proprietary" label. In other words, the government recipient is under no obligation to inform the originating company before disclosing the information within the government to another contractor. If the government recipient wants to publicly disclose the information in response to a FOIA request, then the government recipient would have to notify the originating company. Nongovernment personnel can be granted access to proprietary technical data in accordance with current regulations, but DoD needs to clarify with the Office of Federal Procurement Policy, and potentially the DOJ, whether nongovernment personnel can be granted access to nontechnical "proprietary" information. Current, unofficial DoD policy is to grant some nongovernment personnel access to nontechnical "proprietary" information following execution of NDAs, but this procedure is not being applied consistently.

Source Selection Sensitive: Based in statute, 41 U.S.C. 2101. Access privileges are clear.

The label "Source Selection Sensitive," or similar references to "Source Selection," is derived from explicit U.S. law. According to 41 U.S.C. 2101, "The term 'source selection information' means . . . prepared for use by a Federal agency to evaluate a bid or proposal to enter into a Federal agency procurement contract, if that information previously has not been made available to the public or disclosed publicly." Under 41 U.S.C. 2102, "a person . . . shall not knowingly disclose contractor bid or proposal information or source selection information before the award of a Federal agency procurement contract to which the information relates." These legal provisions are implemented government-wide in 48 CFR 3.104, "Procurement Integrity," which includes repeated use of the term "source selection."

Within DoD, "Source Selection" is also repeatedly used in DoDI 5000.02, *Operation of the Defense Acquisition System*, which includes the process for selecting a contractor. The most detailed description of how to *handle* "Source Selection" information is contained in the source selection procedure issued by the Director, Defense Procurement and Acquisition Policy (DPAP) within OUSD(AT&L). The procedure states:

1.4.1.2.6. Ensure that all persons receiving source selection information are instructed to comply with applicable standards of conduct (including procedures to prevent the improper disclosure of information) and sign a Non-Disclosure Agreement and a conflict of interest statement. Ensure Conflict of Interest Statements (from both Government members/advisors and non-Government team advisors) are appropriately reviewed and actual or potential conflict of interest issues are resolved prior to granting access to any source selection information.¹¹

"Source Selection" appears to be appropriate for use on DoD documents, and access privileges appear to be understood. The label needs to be applied by the document creator or

¹¹ Shay D. Assad, "Department of Defense Source Selection Procedures," memorandum, Washington, D.C.: Director, Defense Procurement and Acquisition Policy, Acquisition, Technology and Logistics, Department of Defense, March 4, 2011.

organization entering information into a government system. Access can be granted to government and nongovernment personnel, as needed.

Technical Distribution Statements: Basis in DoD policy (DoDI 5230.24). Using the label is appropriate, and additional access can be granted by the document controller as needed.

“Technical Distribution Statements” (sometimes called “Distribution Statements on Technical Documents” and frequently abbreviated as “Distribution Statements”) are required to be applied to “[a]ll newly created, revised, or previously unmarked classified and unclassified DoD technical documents.”¹² According to DoDI 5230.24, “All DoD Components generating or responsible for technical documents shall determine their distribution availability and mark them appropriately before primary distribution. Distribution statements shall be used in addition to applicable classification and dissemination control markings.”¹³ Unlike most of the other CUI labels discussed in this report, distribution statements have explicit definitions and procedures for use in official DoD policy. Also, the labels themselves provide clear guidance about who is allowed to view the contents of the labeled document. As a result, the authors did not encounter any instances of DoD personnel misunderstanding distribution statements.

There are six possible distribution statements:

- “DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.”
- “DISTRIBUTION STATEMENT B. Distribution authorized to U.S. Government agencies only (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).”
- “DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government agencies and their contractors (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).”
- “DISTRIBUTION STATEMENT D. Distribution authorized to the Department of Defense and U.S. DoD contractors only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).”
- “DISTRIBUTION STATEMENT E. Distribution authorized to DoD Components only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).”
- “DISTRIBUTION STATEMENT F. Further dissemination only as directed by (inserting controlling DoD office) (date of determination) or higher DoD authority.”¹⁴

As shown above, the distribution statements clearly delineate the personnel permitted to view the labelled document. Distribution Statements B and C include all of the U.S. government, while D and E include only DoD. Further, the distribution statements clearly differentiate between government personnel and government contractors, and the “controlling DoD office” for the document can be contacted to request distribution beyond the distribution statement limit.

¹² DoDI 5230.24, p. 10.

¹³ DoDI 5230.24, p. 10.

¹⁴ DoDI 5230.24.

It is possible that a document with a distribution statement could have additional labels on it, such as “PROPIN.” In that case, additional procedures might have to be followed to allow access after the controlling DoD office approves.

Findings

Our assessment of these commonly used CUI markings strengthens the findings of our earlier work.¹⁵ Current practice tends to rely on past practices to determine data management and handling procedures. While a host of labels are available, the actual use, handling, and ultimate labeling of data tends to be driven by prior practices that do not represent current policy. It is unsurprising that, given current policy’s confusing, unclear, incomplete, and potentially conflicting guidance, the acquisition workforce has decided to stick with established practice rather than to sort through dense policies on handling a wide variety of data requiring protection.

Overall, there is no central program that captures all CUI data labels and that both defines and establishes proper handling procedures. This means that there is no central reference that ensures that labels are placed correctly on material. There is no checking function to monitor that labels are correctly applied, and there is no appeals function to allow users to question data labeling. This lack of oversight also applies to situations in which data labels are missing: There is no established procedure for identifying and responding to data that lack a CUI marking.

The result of this set of mismatched policies is the likely excessive use of labels and mislabeling of CUI material. Although we found that many of the most commonly used CUI labels have a basis in law or policy, this basis does not ensure that labels are understood or properly used in practice or that the labels establish clear handling procedures.

Proper access to data, both within the government and between the government and contractors or FFRDCs, can be unnecessarily restricted because of bureaucratic inertia and fear of repercussions from sharing otherwise protected data. A more robust, central program for CUI data labeling, access, training, and management (including monitoring and challenging document originators) may help to facilitate smoother sharing and protection of CUI within DoD, which will ultimately improve the efficiency and effectiveness of DoD analysis and oversight.

¹⁵ Riposo et al., 2015.

Security Policy and Its Implications for AIR and DAMIR

In Chapters Two and Three, we reviewed proprietary information and commonly used distribution labels or markings on acquisition data. In this chapter, we examine how security policies affect OUSD(AT&L)'s ability to provide efficient and secure access to acquisition data, focusing on implementation challenges associated with those policies. Given the vast number of policies governing data sharing, access, and management in DoD, as well as sponsor interest as an acquisition data manager,¹ we focus on how OUSD(AT&L) personnel manage the AIR and DAMIR information systems. We also document some of the effects of the introduction and implementation of security policies on these systems.

Background

In our earlier work, we found that “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.”² In addition, “the policy landscape governing information sharing is vast and decentralized. . . . [D]ecentralization has made it more difficult for individuals to locate information or guidance of a particular nature, or to identify the organization responsible for providing such guidance.”³

Our earlier work also found that while the policy environment governing information systems results in inefficiencies, it does not prevent accomplishment of an individual's work or an organization's mission within DoD. Additionally, the consequences of poor data access and information sharing—such as lower-quality analysis or ill-informed decisions—are extremely difficult to precisely evaluate.

The security policy environment is one in which many DoD and other government organizations are promulgating security policy on overlapping and interrelated topics. The need for security policy to respond to rapidly evolving technology complicates this environment further. As a result, many security policies are relatively new or frequently changing. Finally,

¹ ARA/EI's mission is to “[p]rovide leadership timely access to accurate, authoritative and reliable data supporting acquisition oversight, analysis, and decision-making by identifying information management and capability needs on behalf of the USD(AT&L) and obtaining, managing, and delivering Acquisition data and analytical capabilities in support of OUSD(AT&L) strategic Acquisition priorities and initiatives.”

² Riposo et al., 2015, p. 33.

³ Riposo et al., 2015, p. 2.

DoD's new CUI program, which is based on federal policy and is led by the National Archives, has not been finalized.⁴

The challenges that this environment poses for information managers include

- understanding the breadth of policies that must be addressed for compliance
- finding funds and technical capability to implement new policies or changes to existing policies
- developing mechanisms for evaluating costs and benefits of new security policies—and to determine exceptions to them
- ensuring that CUI is properly identified, marked, and protected.

AIR and DAMIR information system managers must deal with the effects of this complicated environment while attempting to balance the need for information security with the utility of these two information systems and as directed by statute, regulation, and policy.

The overall purpose of AIR is to provide one central, easily accessible location for all MDAP and MAIS acquisition documents in support of oversight and decisionmaking. More specifically, AIR stores “final milestone documents for Pre-Major Defense Acquisition Programs, Unbaselined Major Automated Information Systems, Acquisition Category (ACAT) ID, ACAT IAM, and Special Interest Programs with potential to expand to include ACAT IC and IAC programs later.”^{5, 6} AIR largely represents the changes associated with management of unstructured data (i.e., documents).

DAMIR serves several key functions, including reporting; storage; quality assurance; analysis; oversight; and tracking cost, schedule, and performance of major acquisition programs. OUSD(AT&L)/ARA notes that DAMIR

is a DoD initiative that provides enterprise visibility to Acquisition program information. DAMIR streamlines acquisition management and oversight by leveraging web services, authoritative data sources, data collection, and data repository capabilities. DAMIR identifies various data sources that the Acquisition community uses to manage Major Defense Acquisition Programs (MDAP) and Major Automated Information Systems (MAIS) programs and provides a unified web-based interface through which to present that information. DAMIR is the authoritative source for Selected Acquisition Reports (SAR), SAR Baseline, Acquisition Program Baselines (APB), and Assessments. It is a powerful reporting and analysis tool with robust data checks, validation, standardization and workflow leveling. It has extensive security capabilities as well as both classified and unclassified versions. One component of DAMIR, Purview, is an executive information system that displays program information such as mission and description, cost, funding and schedule. It is OSD's solution for structured acquisition data presentation and uses web services to obtain and

⁴ U.S. Department of Defense Manual 5200.01, Vol. 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)*, February 24, 2012, pp. 1–2.

⁵ Frank Kendall, *Acquisition Information Repository Implementation Guidance*, September 25, 2012, p. 1.

⁶ ACAT ID, IAM, IC, and IAC are categories of acquisition programs by dollar value, by what is being acquired, and by decision authority. See Defense Acquisition University (2016) for additional information on the categories of acquisition programs.

display Defense Acquisition Executive Summary (DAES) data directly from the Service acquisition databases.⁷

DAMIR represents the challenges associated with managing a repository of structured data that both pulls data from information systems (e.g., Federal Procurement Data System–Next Generation and the Air Force System Metric and Reporting Tool) and also pushes structured data to other information systems (e.g., Cost Assessment Data Enterprise).

We used discussions with the information managers for AIR and DAMIR and policy analysis to identify and analyze problems related to implementing security policy for these two information systems. Our first step was to understand the security structure of these systems. Key topics in our discussions on the information systems included

- technical and nontechnical requirements driven by security policy and procedure
- AIR and DAMIR security strategies
- specific security policies, processes, and procedures on how the information managers build, manage, operate, and grant access to these systems
- procedures for determining user access.

Our discussions also focused on identifying challenges or problems related to security policies, such as

- problems encountered with granting access or managing access to the information system
- problems that arise when the owner of the system is not also the host of the system
- specific security policies that have required significant resources to implement
- the ability to request waivers or exemptions to security policies if they are deemed not relevant or too costly to implement
- challenges funding the implementation of new policies.

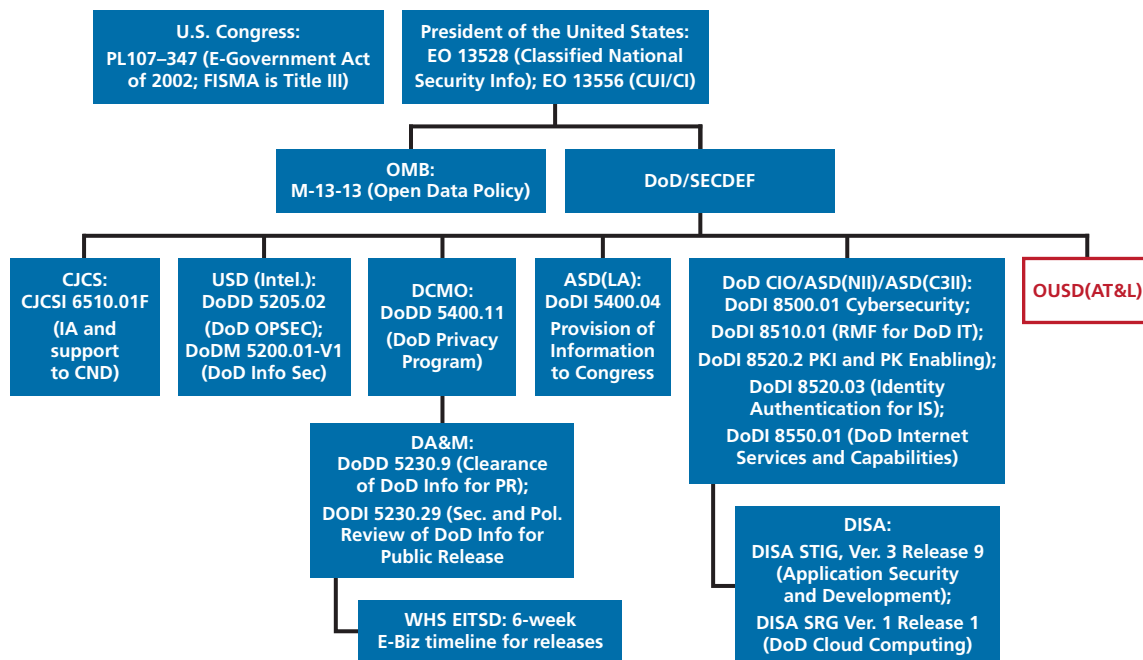
Security Policies Identified Through Discussions

The information system managers identified a multitude of security policies affecting management and operation of the information systems. Figure 4.1 shows the hierarchy of organizations issuing these policies. The policies originate at all levels of DoD, from the Under Secretary or Assistant Secretary level to the local organization that hosts and manages information systems for government agencies. Security-related policies also emanate from outside DoD, including the Office of the President (executive orders), the Office of Management and Budget (directives), and Congress (statute). OUSD(AT&L), which is responsible for setting acquisition policy and performing oversight, does not issue any of the security-related policies affecting AIR and DAMIR. However, OUSD(AT&L) does issue the policies determining the information stored in those systems.

The fact that the OUSD(AT&L) information system managers must implement security policies that originate elsewhere is fundamental to the challenges and issues that AIR and DAMIR managers and users experience. Information security policy is written for general

⁷ Defense Acquisition Management Information Retrieval (DAMIR) information system, “Welcome to DAMIR Web-Help,” OUSD(AT&L) ARA Directorate, undated.

Figure 4.1
Hierarchy of Organizations That Issue Security Policies



SOURCE: Author discussions with AIR and DAMIR information managers.

NOTES: ASD(C3I) = Assistant Secretary of Defense (Command, Control, Communications, and Intelligence); CJCSI = Chairman of the Joint Chiefs of Staff Instruction; DA&M = Director of Administration and Management; DCMO = Deputy Chief Management Officer; DISA = Defense Information Systems Agency; OPSEC = Operations Security; STIG = Security Technical Implementation Guide.

RAND RR1476-4.1

application across DoD or the government. AIR and DAMIR contain very specific kinds of information in support of OUSD(AT&L) functions, including decisionmaking and analysis. Implementation is thus characterized by the need to interpret the policy and apply it to a specific information system. This illustrates the inherent tension between the need to protect both information systems and the data they contain and the business or use case⁸ of the information system. Striking an appropriate balance is perhaps the fundamental management challenge.

Table 4.1 lists the key security-related policies with which AIR and DAMIR must comply, as identified in discussions with AIR and DAMIR information managers. Policies range from executive orders to public laws to specific DoD directives, instructions, and manuals. The policies cover a wide range of security-related topics affecting information system governance, access, markings, protection, and other subjects. Some of the policies have changed over time. For example, the Risk Management Framework (RMF) has replaced the DoD Information Assurance Certification and Accreditation Process. None of these policies were written for AIR or DAMIR, but AIR and DAMIR managers must comply with all of these policies or risk disconnection from the network. As a result, compliance with security policy takes precedence over other needs, such as adding capability.

⁸ In other words, how the information is used.

Table 4.1
Security Policies Affecting AIR and DAMIR

Name	Subject	Issuer	Date	Notes
Executive Order 13526	Classified National Security Information	President of the United States (POTUS)	December 29, 2009	Prescribes a uniform system for classifying, safeguarding, and declassifying national security information
Executive Order 13556	Controlled Unclassified Information (CUI) and/or Critical Information (CI)	POTUS	November 4, 2010	Establishes an open and uniform program for managing unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies
Public Law 107-347	E-Government Act of 2002; FISMA is included in this act as Title III	U.S. Congress	December 17, 2002	Enhances management and promotion of electronic government services and processes
M-13-13	Open Data Policy-Managing Information as an Asset	Office of Management and Budget	May 9, 2013	Establishes a framework to help institutionalize the principles of effective information management at each stage of the information's life cycle to promote interoperability and openness
CJCSI 6510.01F	IA and Support to Computer Network Defense (CND)	Chairman of the Joint Chiefs of Staff	February 9, 2011; Revised: October 10, 2013	Provides joint policy and responsibilities for Information Assurance (IA) and support to CND
DoDD 5205.02	DoD Operations Security (OPSEC) Program	USD(I)	March 6, 2006	Updates policy and responsibilities governing DoD OPSEC
DoDM 5200.01, Vol. 1	DoD Information Security Program: Overview, Classification, and Declassification	USD(I)	February 24, 2012	Describes the DoD Information Security Program
DoDD 5400.11	DoD Privacy Program	DCMO	October 29, 2014	Updates the established policies and assigned responsibilities of the DoD Privacy Program
DoDI 5400.04	Provision of Information to Congress	Assistant Secretary of Defense (Legislative Affairs)	March 17, 2009	Implements the policies and procedures of DoD's provision of information, both classified and unclassified, to Congress; Note: affects SARs
DoDI 5200.40	DoD Information Technology Security Certification and Accreditation Process	ASD(C3I)	December 30, 1997	Implements policy, assigns responsibilities, and prescribes procedures for certification and accreditation of IT
DoDI 8500.01	Cybersecurity	DoD CIO	March 14, 2014	Establishes a DoD cybersecurity program to protect and defend DoD information and information technology; adopts the term "cybersecurity"

Table 4.1—continued

Name	Subject	Issuer	Date	Notes
DoDD 8500.01E	Information Assurance (IA)	ASD(NII)/ DoD CIO	October 24, 2002	Establishes policy and assigns responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology and supports the evolution to network-centric warfare
DoDI 8500.2	Information Assurance (IA) Implementation	ASD(C3I)	February 6, 2003	Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks; incorporated into and canceled upon issuance of DoDI 8500.01 on March 14, 2014
DoDI 8510.01	Risk Management Framework (RMF) for DoD Information Technology (IT)	DoD CIO	March 12, 2014	Replaces the DoD Information Assurance Certification and Accreditation Process, established on November 28, 2007. Establishes the RMF for DoD IT, establishing associated cybersecurity policy and assigning responsibilities for executing and maintaining the RMF
DoDI 8520.2	Public Key Infrastructure (PKI) and Public Key (PK) Enabling	ASD(NII)	April 1, 2004	Implements policy, assigns responsibilities, and prescribes procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption
DoDI 8520.03	Identity Authentication for Information Systems	ASD(NII)/ DoD CIO	May 13, 2011	Assigns responsibilities and prescribes procedures for implementing identity authentication of all entities to DoD information systems
DoDI 8550.01	DoD Internet Services and Internet-Based Capabilities	DoD CIO	September 11, 2012	Replaces Web Site Administration Policies & Procedures (WAPP), established on January 11, 2002; establishes policy, assigns responsibilities, and provides instructions for DoD Internet services on unclassified networks
DoDD 5230.9	Clearance of DoD Information for Public Release	DA&M	August 22, 2008; revised March 16, 2016	Updates policy and responsibilities for the security and policy review process for the clearance of official DoD information proposed for official public release by DoD and its employees
DoDI 5230.29	Security and Policy Review of DoD Information for Public Release	DA&M	August 13, 2014	Assigns responsibilities and prescribes procedures to carry out security and policy review of DoD information for public release
DoD Cloud Computing Security Requirements Guide (SRG), Version 1, Release 1	DoD Cloud Computing Security Requirements Guide	DISA	January 12, 2015	Documents cloud security requirements in a construct similar to other SRGs published by DISA for DoD

Table 4.1—continued

Name	Subject	Issuer	Date	Notes
DISA STIG, Version 3, Release 9	DISA Application Security and Development Security Technical Implementation Guide	DISA	October 24, 2014	Possible new policy that prohibits using real data in a test environment
Guidebook	DoD Guidebook for CAC-Eligible Contractors for Unclassified Network Access	DPAP	November 21, 2014	Pulls together multiple policies governing network access
Other policy	Six-week timeline for releases	Washington Headquarters Services, Enterprise Information Technology Services Directorate (WHS EITSD)	Specific policy date is unavailable	DAMIR information managers follow the WHS EITSD timeline for any changes that need to be made to DAMIR (e.g., software releases)

SOURCES: Discussions and input from AIR and DAMIR stakeholders.

NOTE: CAC = Common Access Card.

A closer look at the security policies listed in Table 4.1 shows that they cover a broad set of topics and information, including

- website administration policies and procedures
- certification and accreditation procedures
- PKI procedures and requirements
- CUI labeling and protection
- risks associated with aggregation of CUI
- operational security programs protecting both classified information and CUI
- access policy and procedures
- review and clearance of information for public release
- information assurance and dissemination
- identity authentication
- requirement for an information security strategy
- privacy and confidentiality (personally identifiable information)
- use of real data in a test environment
- account deletion after period of dormancy
- data sharing and passing credentials across information systems
- authorizing official (AO) designation and responsibilities.

Many policies address more than one area, and policies have overlapping topics. While new policies are routinely circulated among key stakeholders as drafts to elicit feedback, the complexity of the policy environment can result in conflicting direction or guidance to information managers and owners. Information managers must interpret each policy and apply it to a specific case. To the extent that policies are either not relevant or do not fit the informa-

tion systems' business case,⁹ waivers or exemptions must be sought by the information managers. However, there is no formal, consistent institutional structure or process for managing the risk inherent in balancing security with utility.

One possible policy conflict concerns the AO. The AO is a critical position affecting policy implementation. The AO is the decisionmaker for each information system, interpreting security policy and deciding how it applies to a specific information system. The recently released *Risk Management Framework (RMF) for DoD Information Technology (IT)* (DoDI 8510.01, March 12, 2014) illustrates the conflicts in security policies. Subsection c: Tier 3—IS (Information Systems) and Platform Information Technology (PIT) Systems, reads in part:

- (1) AO. The DoD Component heads are responsible for the appointment of trained and qualified AOs for all DoD ISs and PIT systems within their Component. AOs should be appointed from senior leadership positions within business owner and mission owner organizations (as opposed to limiting appointments to CIO organizations) to promote accountability in authorization decisions that balance mission and business needs and security concerns.
- (7) OSD Systems. Pursuant to DoDD 5105.53 (Reference (x)), the Director of Administration and Management is responsible for the IT, including IS and PIT systems, supporting the OSD staff in the National Capital Region.

The new policy (DoDI 8510.01, 2014) encourages the AO to balance mission and business needs, but the old policy (DoDD 5105.53, 2008) identifies the Director of Administration and Management as responsible for OSD IT systems. The new policy clearly states that the AO should be a senior official within the mission area that the information system supports. Yet that same policy makes the director of administration and management—a generalist—responsible for the information system. The language used in the two policies creates ambiguity; it points to two different individuals in two different organizations with responsibility for information security of a specific system. Mission-oriented officials might be expected to find some security risks acceptable in order to preserve the utility of the system. An official whose mission is largely security might not agree.

Description of Key Attributes

We used the AIR and DAMIR information systems as case studies to examine the implications of implementing security policies. The information in the discussion below comes from discussions with database owners and managers, our familiarity with the systems as users,¹⁰ and a review of system documentation.

The characteristics of an information system affect implementation of security policies. Security policies are written broadly to apply to all covered systems; actual implementation requires interpreting and operationalizing those policies in a way suitable for a specific system. As a result, basic characteristics of information systems—data content, data owner, system

⁹ EI 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” (OUSD(AT&L)/ARA, undated). 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.

¹⁰ Several of the authors have access to and familiarity with at least one of these information systems.

manager, AO—have implications for how security policy is applied to a specific information system.

Table 4.2 summarizes key characteristics of AIR and DAMIR that affect implementation of security policies for those systems. Though both systems support the acquisition oversight function, differences in specific purpose, data content, AO, and host result in different implementation challenges.

AIR was chartered by OUSD(AT&L) in 2012.¹¹ It can be accessed by both Non-classified Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet). AIR is a repository for documents. It contains the formal, approved acquisition program documentation required by DoDI 5000.02 for MDAPs and MAISs. In other words, the “data” in AIR are specific program documents (reports, certifications) required by policy and used to inform acquisition decisionmaking and oversight. The organizations that developed these documents, typically program offices or functional offices within OSD, own them for

Table 4.2
Basic Characteristics of AIR and DAMIR Information Systems

	AIR	DAMIR
Year started	2012	2004–2005
Content	Unstructured data: acquisition information required by the current DoDI 5000.02 (46 information requirements) and an Acquisition Decision Memorandum by USD(AT&L)	Structured data: SARs, MAIS Annual Report, APBs, DAES, Project Objective Memorandum (POM), Budget Estimate Submission, President’s Budgets, top-level earned value data
Function	Acquisition oversight	Acquisition oversight
Access adjudicator	Document owner	ARA
Repository manager	ARA	ARA
Repository host	Defense Technical Information Center (DTIC)	DoD WHS/EITSD
AOs	DTIC	DoD Joint Service Provider (JSP)
Access procedures	Verification of user’s identity and need to know the information, with a government sponsor indicated on DD 2875. DoD CAC/ PKI is required. A .mil email account is required.	Account is requested through organizational trusted agent point of contact. CAC/PKI and external certificate authority are also needed. ^a
Reasons for restriction	CUI (varies)	CUI (mostly FOUO)
Groups with access	DoD government and nongovernment employees	DoD government and nongovernment employees; Congress
User statistics	850	Approximately 6,000

SOURCES: Compiled by RAND from discussions with AIR/DAMIR information managers.

^a DoD’s External Certification Authority (ECA) program “is designed to provide the mechanism for these entities to securely communicate with the DoD and authenticate to DoD Information Systems” (Information Assurance Support Environment, 2016).

¹¹ Kendall, 2012, p. 1.

purposes of access control and markings. OUSD(AT&L)/ARA owns the information system, which resides on a server at DTIC. DTIC, which is part of OUSD(AT&L), is also the AO, and so DTIC determines how security policy applies to the system.

The DAMIR system, released in 2005, resulted from a decades-long OSD effort to make program-level status reporting and outcome tracking consistent over time and across Services and programs. The DAMIR system has both unclassified (accessed via NIPRNet) and classified (accessed via SIPRNet) versions. The current version of DAMIR supports the generation, distribution, and archiving of SARs, as well as information supporting the DAES process. It also includes higher-level earned-value management (EVM) data.¹² DAMIR has specific defined data elements using data collected and generated throughout the acquisition process by DoD that can be combined and analyzed in multiple ways by users serving multiple functions. It is a much more complex and larger database than AIR. It receives direct input from the Services and feeds other DoD information systems. DoD WHS/EITSD is the host, while JSP is the AO for DAMIR, though the data are owned by multiple acquisition organizations and managed by an OUSD(AT&L)/ARA support contractor.

AIR: Implications and Challenges for Implementing Security Policy

Business rules for AIR, including access procedures, are partly an interpretation of security policies. The AIR information managers have created a set of business rules based on their interpretation of those policies. For instance, according to DoD Manual 5200.01, Vol. 4 (2012), “The 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.”¹³ 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 inconsistencies in the marking of the documents. The AIR managers attribute these inconsistencies to the variety of security classification guides being used to mark documents by the originators.

For some markings (e.g., Source Selection Sensitive and Proprietary), AIR prompts owners to add the date when markings are no longer necessary (most default to ten years). There is no process for ensuring that up-to-date marking conventions are followed appropriately for each document uploaded to AIR.

Based on our experience and our interpretation of security policies, AIR management and use by nongovernment employees is complicated by the need to access AIR on an IT system

¹² According to the PARCA Earned Value Management division in the Office of the Assistant Secretary of Defense for Acquisition (Earned Value Management, home page, undated):

Earned Value Management (EVM) is one of DoD's and industry's most powerful program planning and management tools. The purpose of EVM is to ensure sound planning and resourcing of all tasks required for contract performance. It promotes an environment where contract execution data is shared between project personnel and government oversight staff and in which emerging problems are identified, pinpointed, and acted upon as early as possible. EVM provides a disciplined, structured, objective, and quantitative method to integrate technical work scope, cost, and schedule objectives into a single cohesive contract baseline plan called a Performance Measurement Baseline for tracking contract performance.

¹³ U.S. Department of Defense Manual 5200.01, Vol. 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)*, Washington, D.C., February 24, 2012, p. 9.

approved through Defense Security Service (DSS) inspection, using a .mil email address associated with a CAC, and with approval of a government sponsor.¹⁴ The DSS-approved IT system reflects specific technical protection of the system and its data. This means that documents cannot be passed to another system, though such ability would enhance the value of the system for analysis. A CAC is used to validate a user's identification.

The government sponsor provides the rationale for granting a user access to AIR for a specific purpose. The permissions process is separate from the sensitivity of documents stored in AIR. The policy assigning authority to grant access to the data owner allows for denial of access for reasons other than security.¹⁵

DAMIR: Implications and Challenges for Implementing Security Policy

DAMIR is managed by the OUSD(AT&L)/ARA/EI office. It is hosted by WHS EITSD, which partially reports to OUSD(AT&L)/ARA and also to JSP. JSP does not reside within OUSD(AT&L).¹⁶ JSP has an important role involving security policy: It is the AO for DAMIR. According to DoDI 8510.01 (March 12, 2014), the AO is "responsible for authorizing the system's operation based on achieving and maintaining an acceptable risk posture."¹⁷ Based on discussions with information managers, the external host/AO structure minimizes flexibility in managing DAMIR. This may lead to a disconnect between the business case¹⁸ for data use and security policies because the AO resides outside of the organization of OUSD(AT&L) and is not a user or maintainer of the data in the system. The AO is responsible for interpreting security-related policies applicable to DAMIR. Understanding the business case for DAMIR is critical to balancing implementation of security policies between achieving the intent of those policies and not overly constraining the utility of the system to its users.

The DAMIR system owner, OUSD(AT&L)/ARA, grants permissions; there is a point of contact for each organization (e.g., the Office of Cost Assessment and Program Evaluation, PARCA) with individuals requesting access. This government point of contact is responsible for verifying the need for access. Permissions also govern portions of the site accessible to users.

DAMIR has evolved significantly over time, increasing and improving its functionality for users. In practice, that means additional lines of code and even changes in the way that certain functions are accomplished. To ensure that these updates work properly and do not

¹⁴ A government sponsor verifies to the AIR and DAMIR information managers that a nongovernment user has a valid "need to know" in order to access the information.

¹⁵ Kendall, 2012, p. 1.

¹⁶ According to an Office of the DoD CIO and DCMO Memorandum (April 3, 2015), p. 2:

By 20 July 2015, DISA in partnership with the Pentagon IT Study Group will establish a Pentagon DISA Field Service Activity referred to as the Joint Information Technology Service Provider-Pentagon (JITSPP). The Deputy Chief Management Officer (DCMO) will have interim funding and resources review, and oversight of the JITSPP with the Department of Defense Chief Information Officer (DoD CIO) providing technical oversight until the JITSPP reaches full operational capability as a field service activity.

After this initial guidance, the name was changed from JITSPP to JSP.

¹⁷ DoDI 8510.01, March 12, 2014, p. 3.

¹⁸ In other words, how the information is used for analysis and decisionmaking.

adversely affect other functions, the IT support contractors¹⁹ assisting with management of the system need to test the updates with representative data. One security-related policy states that real data cannot be used to test the system. This requires programmers to invent data to test the system, a job made difficult by the complexity of the information in DAMIR, its connections to other systems for input and output, and its wide range of uses. Not using actual data to test the system also results in uncertainty as to whether the new programming works with no unanticipated consequences.

A security policy that requires accounts to be disabled after 30 days of inactivity has had a significant effect on DAMIR.²⁰ Many of DAMIR's users, such as congressional staff and FFRDC analysts, login infrequently, such as when new SAR or DAES reports come out or when analysts require specific data. As a result, DAMIR accounts are often suspended or terminated. According to the information managers, the DAMIR team has been required to re-register about 30 percent of 4,000 active users, meaning that one DAMIR accounts manager spends at least one day per week on re-registration. There are costs associated with a system like DAMIR losing users, such as delays in conducting analyses and obtaining data to inform decisions when waiting for access to be restored.

Authorization-to-Operate (ATO) status requires renewal every three years.²¹ Making changes to the system may result in it having to undergo the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) process again, or the system may lose ATO status. This poses a problem for an IT system that evolves over time.

Implementing new policies within the complex system that is DAMIR (which currently has more than 1.5 million lines of code) is challenging. DAMIR was implemented under previous security-related policies, and adapting its structure, programming, and business rules to accommodate new policies is a nontrivial task. There is no up-to-date security architecture document because architecture and security policies governing DAMIR have evolved independently. Similarly, new interpretations of existing policies have consequences. For example, a new interpretation of what constitutes personally identifiable information forced a Privacy Impact Assessment.²² In addition, because the DAMIR AO is separate from its managers,

¹⁹ CACI Inc.

²⁰ CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*, Washington, D.C., February 9, 2011, current as of June 9, 2015.

²¹ DoD, "Department of Defense Information Assurance Certification and Accreditation," Personnel and Readiness Information Management, undated:

The Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) is a process by which information systems are certified for compliance with DoD security requirements and accredited for operation by a designated official. DIACAP provides visibility and control for the secure operation of DoD information systems.

In 2014, the Risk Management Framework replaced DIACAP. The example provided to us in our discussions with the information managers involved the DIACAP process.

²² According to DoDI 5400.16:

It is DoD policy that PIAs are:

a. Completed on DoD Information Technology (IT) and electronic collections that collect, maintain, use, or disseminate PII [personally identifiable information] to:

(1) Ensure PII handling conforms to applicable legal, regulatory, and policy requirements regarding privacy.

(2) Determine the need, privacy risks, and effects of collecting, maintaining, using, and disseminating PII in electronic form.

DAMIR managers must work around the AO's schedule for the implementation of patches, rather than a schedule that is tailored for DAMIR implementation and linked with planned upgrades. Finally, service-level information systems also feed information to DAMIR, which creates additional layers of scheduling and policy interpretation issues.

Impacts of Security Policies

OUSD(AT&L) has no formal measurement system for tracking the costs and level of effort required to comply with security-related policies. Such a system might measure labor hours associated with implementation (e.g., programming time, re-registering user accounts, and recertification). Other, less-quantifiable metrics might include delays in access to databases and constraints on information use.

It is possible to link specific policies to the resources required to implement them. Table 4.3 estimates these requirements for AIR and DAMIR. Resources required are expressed as a level-of-effort metric (e.g., a person-month or person-year). While these are rough estimates, they do indicate that compliance can require significant effort for the unfunded requirement of security-related policy implementation.

Table 4.4 illustrates impacts attributable to the overall security-related policy environment. These impacts cannot be clearly tied to a specific policy but instead reflect general level-of-effort estimates for policy implementation.

Findings

The information security environment is characterized by

- multiple organizations promulgating policy on overlapping and interrelated topics
- the need to respond to rapidly evolving technology, resulting in frequent revisions to security policies that must be implemented by information managers as unfunded requirements
- the need to appropriately balance the application of security policy with the business or use case of each information system.

Policies originate outside of OUSD(AT&L) and tend to be one-size-fits-all; they do not take the unique characteristics of each system into account. Some policies appear to duplicate the guidance found in other policies, with no centralized, coordinated effort to deconflict policies and ensure consistent interpretation and appropriately tailored implementation. Policy originators or owners do not fund compliance activities, so new or changed policy is effectively

(3) Examine and evaluate protections and alternative processes to mitigate potential privacy risks.

b. Performed when PII about members of the public in accordance with Reference (c), DoD personnel, contractors, or foreign nationals employed at U.S. military facilities internationally, is collected, maintained, used, or disseminated in electronic form.

c. Performed on DoD IT and electronic collections including those supported through contracts with external sources that collect, maintain, use, or disseminate PII about members of the public, DoD personnel, contractors, or in some cases foreign nationals.

Table 4.3
Estimated Impacts of Security Policies

Name	Subject	DAMIR/AIR Application	Qualitative Effects	Resources Required (approximate)
Executive Order 13556	Controlled Unclassified Information (CUI) and/or Critical Information (CI)	Implement security markings for DAMIR reports and views	Internal debate regarding how to appropriately label documents	Currently unquantified, but a major effort
DoDI 8520.2	Public Key Infrastructure (PKI) and Public Key (PK) Enabling	PKI implementation at DTIC to support AIR/ DAMIR integration	Required a setting change for Site Minder ^a	1 person-month
CJCSI 6510.01F	IA and Support to Computer Network Defense (CND)	EITSD enforces a lockout policy if the account is not used every 30 days.	Drafted business case analysis against implementation (denied); E-Biz implemented macros with bugs; user base and DAMIR permissions personnel had significant problems for several months.	1 full-time equivalent (FTE) per year
DISA STIG, Version 3, Release 9	DISA, Application Security and Development Security Technical Implementation Guide	No live data permitted in non-production environments.	Security policy change/enforcement created the mandatory requirement for “representational data” that had to be reverse engineered or manufactured from scratch.	Initial: 3.5 person-months per year; Sustainment: 0.5 person-months per year

SOURCES: Input from AIR and DAMIR stakeholders.

^a Site Minder helps manage access to applications.

an unfunded requirement for system managers. There is also a perception that the business case analyses that attempt to explain how the data are used are not given sufficient weight in implementation and compliance decisions. Together, these characteristics of the security policy environment suggest that there is no coherent institutional structure supporting information system managers as they attempt to interpret and implement policy.

Implementation challenges, shared by many information system managers, include

- understanding the breadth of policies that need to be addressed for compliance
- finding funds and technical capability to implement new policies as they are created
- developing mechanisms for evaluating costs and benefits of new security policies to determine exceptions and better balance security risks with the use case for a specific information system
- making sure that CUI is properly identified, marked, and protected.

This analysis of how security policies affect the management of AIR and DAMIR found that the implementation of information security policies results in costs to system managers, hosts, and users, as well as inefficiencies that adversely affect acquisition analysis and decision-making. Nevertheless, we found no evidence that missions are not being accomplished, or that decisions are based on incomplete information because that information cannot be accessed in a timely manner. But we also found that DoD lacks a mechanism by which the costs and

Table 4.4
Estimated Impacts of General Security Policy Implementation

DAMIR/AIR Application	Resources Required (approximate)
The OUSD(AT&L) SharePoint requires extra registration. Most of the effort for requesting an account is required of the external user, who must complete the external registration process.	No estimate given
Siena integration for DAMIR: Siena is a software integration task that allows DAMIR to extract CAC information from the Defense Manpower Data Center's milConnect web site. This integration task did not include resources for the actual deployment.	1 FTE for 3 months
The Internet Explorer 8 (non-supported browser) check requires 1 person-week. This does not include resources for the actual deployment.	1 FTE for 1 week
DoD's policy requires certain activities to be performed by persons with Security+, which is a specific information security certification.	16 person-weeks (8 FTE x 2 weeks)
Security advisories are time-consuming, so the discovery of a major vulnerability can delay system administrators' schedule by several weeks.	1 person-month per year
When new software that has not already been approved by DoD needs to be used for AIR or DAMIR, the process for approving this new software package takes four to six months.	1 person-month
The DoD Certification and Accreditation process, in which information systems are certified for compliance with DoD security requirements and accredited for operation by a designated official, takes a minimum of six months for DAMIR or AIR.	1 person-month

SOURCES: Input from AIR and DAMIR stakeholders.

benefits of compliance with security policy can be tracked and evaluated to ensure that there are no unintended consequences of implementation.

We also found conflicting intents and provisions and duplication of topic areas. There is no central authority (authoritative source) or coordination mechanism for resolving policy conflicts. There are multiple interpretations of policy caused by diffuse decisionmaking and cultural norms of implementing organizations. Policies designed to fit all organizations cannot account for nuances in application that are due to differences in information-system characteristics. Existing information systems designed under different policy environments may have significant problems responding to new policy. In other cases, software changes or other changes in technology may outpace changes in security policy.

The Impacts of Security Policies on Information Systems Are Difficult to Quantify

Unplanned but necessary changes to the security environment (e.g., changes in software) for data within DoD require quick reaction time and, thus, divert resources from system upgrades and other management activities. There is no measurement system or set of metrics for tracking the impact of compliance activities. There are many anecdotes on this, but concrete evidence (e.g., person-hours spent) is difficult to collect.

The cumulative effects of security policy requirements may be still greater than what is documented for AIR and DAMIR. Compliance actions for these systems may affect other information systems and their users as well.

Conclusions and Options

Our evaluation of how marking and labeling CUI procedures, practices, and security policy affect access to acquisition oversight data resulted in a set of findings for the three main topics that we explored in detail.

Proprietary Information

In regard to the sharing and handling of PROPIN, significant confusion exists within DoD about what information is truly proprietary—and therefore restricted—who can have access to the information, and how to grant access when needed, despite some policies that attempt to define PROPIN and handling restrictions. The current patchwork of law, regulation, and policy inhibits DoD's ability to use nongovernment support, restricts the flow of information, and limits analyses of available data. The PROPIN situation is further complicated by apparent shifts over time in how some nongovernment entities are categorized.

There are several different sources of law and policy that attempt to define and govern PROPIN. Some of these are clear, but others are less specific. Some seem to suggest limitations to the use of the PROPIN label, while others seem to permit indiscriminate labeling of privately owned data as “proprietary” and, therefore, restricted.

Ultimately, based on the researchers' understanding of current practice, the company submitting nontechnical data to the government is responsible for asserting that certain portions are proprietary, but the government recipient is responsible for initially determining whether to accept that assertion and maintaining the “proprietary” label. For public disclosure, the government would have to inform the company-submitter of a determination that all or part of the submission is not proprietary, giving the company-submitter a chance to file a lawsuit to stop disclosure—referred to as a “reverse FOIA” case. However, the procedure for allowing internal support contractors access to the company-submitter's information is less clear. If the responsible government official determines that the information is not proprietary, the government official may not be obliged to inform the company-submitter of the determination. To remain consistent, DoD officials may find it advisable to inform companies that submit data of an initial determination that all or part of the submissions will not be treated as proprietary, along with the justification for that determination.

If the government official wants to publicly disclose the information in response to a FOIA request, then the official would have to notify the originating company. However, true PROPIN can only be disclosed within the government to support contractors (and now

FFRDC employees) when a one-to-one NDA (i.e., an NDA between each individual at the support contractor/FFRDC and each company or program originating data) has been executed.

While the courts have placed the burden on government personnel to make PROPIN decisions, separating PROPIN and non-PROPIN can be difficult with electronic submissions and databases, as well as with the increasing volume of information submitted to DoD.

There is confusion among DoD personnel about who can access PROPIN. PROPIN that is not specifically restricted (e.g., source selection information) can be treated like all other CUI, meaning that all government personnel can be granted access. Yet procedures for granting access to PROPIN vary widely, and decisions to grant or deny access are purely administrative. Ultimately, however, nongovernment entities (e.g., FFRDCs, IT support, SETA support) must gain access to technical data from the prime contractor that is the originator of the information.

Granting access to nontechnical PROPIN may be a more significant challenge. While current laws and policies provide sufficient guidance for granting access to technical data, there is no specific guidance for granting access to nontechnical PROPIN.

The primary distinction among nongovernment entities for purposes of data access and analytic support is between contractors and FFRDCs, but, unfortunately, the law lacks a specific definition for an FFRDC. Multiple federal statutes reference permissible activities for FFRDCs, making clear that they are distinct from other contractors. Nevertheless, recent changes have required FFRDC personnel to secure individual NDAs with each firm for which they wish to review PROPIN, with ad hoc and inefficient tracking of the resulting large number of NDAs.

Origins and Meaning of Commonly Used CUI Acquisition Labels

CUI has a system of markings to demonstrate that the information is sensitive. Yet this set of labels is not as clear, well managed, or well understood as the system surrounding classified information.

Some labeling procedures reflect well-established policies based on current understanding of the law and regulatory environment for data protection and sharing. Others are outdated, legacy markings and practices that are neither current nor accurately updated. Complicating data marking and labeling is the lack of a single document collecting and describing all of these labels (although there are a few core references in DoD policy, such as DoD Manual 5200.01, Vol. 4, *DoD Information Security Program: Controlled Unclassified Information [CUI]*).

Furthermore, data marking and labeling is a process infused with individual judgment and interpretation. The rules in place for data labeling are not always clear and seem rarely to be subject to oversight that would aid standardization.

Overall, the current practice tends to rely on past practices to determine data management and handling procedures. While a host of labels are available, the actual use of them does not represent current CUI policy. This is not surprising, given confusing, unclear, incomplete, and potentially conflicting guidance of current policy.

The result is the likely overlabeling and mislabeling of CUI material. Although many of the most commonly used CUI labels have a basis in law or policy, these labels are not always understood or properly used in practice. This, in turn, means that data, though available, are not effectively and efficiently used to inform, improve, and strengthen acquisition functions.

A more robust central program for CUI data labeling, access, and management (including monitoring and appeals) may facilitate smoother sharing and protection of CUI within DoD.

Security Policy and Its Implications for AIR and DAMIR

Our review of information security policy and how it affects OUSD(AT&L)'s DAMIR and AIR information management systems identified the following challenges:

- understanding the breadth of policies that need to be addressed for compliance
- finding funds and technical capability to implement new policies as they are created
- developing mechanisms for evaluating costs and benefits of new security policies to determine exceptions
- making sure that CUI is properly identified, marked, and protected.

AIR and DAMIR managers must balance the need for information security with utility for users. The resulting tension is fundamental to the challenges and issues that AIR and DAMIR managers and users experience. Information security policy is written for general application across DoD or the government, but AIR and DAMIR contain very specific kinds of information in support of the OUSD(AT&L) functions.

Security policies cover a wide range of topics affecting information system governance, access, markings, protection, and other subjects, and some of the policies have changed over time. None of these policies were written with either AIR or DAMIR in mind, but all must be observed. Consequently, compliance takes precedence over other needs (e.g., adding capability).

Many policies address overlapping areas. The complexity of the policy environment can result in conflicting direction. Information managers must interpret each policy and apply it to a specific case.

Policies tend not to reflect the unique characteristics of each system. Policy originators and owners do not fund compliance activities, meaning that policy changes create an unfunded requirement for system managers. Still, while implementing new information security policies results in costs and inefficiencies, it does not prevent work from being performed.

Security policies for the information systems we reviewed largely originate in multiple offices outside of OUSD(AT&L). To the best of the researchers' knowledge, no evidence exists of a central authority (authoritative source) or coordination mechanism for resolving any resulting policy conflicts.

The impacts of security policies on information systems are difficult to quantify. Additionally, to the best of the researchers' knowledge, no evidence exists of a system for tracking the impacts of compliance activities. There is no shortage of anecdotes, but concrete evidence (e.g., person-hours spent) is difficult to collect.

Options for Improving the Three OUSD(AT&L) Data Issues

Proprietary Data

We identified several policy options that could streamline nongovernment entities' access to PROPIN and improve efficiency and effectiveness of external support. For example, we sug-

gested to DoD personnel that the FAR FFRDC provisions could be revised to declare that FFRDCs are exempt from the NDA requirement or could be covered by a blanket NDA with DoD.

For other contractors, we recommend that DoD consider the following options:

- creating a DFARS provision that would cover nontechnical data,¹ 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.

Legislative and regulatory changes have drawbacks. DoD can propose changes to the DFARS without congressional action, but changing the DFARS would only affect contractors that presently have active DoD contracts. Changing the law would, of course, require congressional action and at least two years—and might result in unwanted changes.

When this report was drafted (January 2016), DoD personnel indicated that they would seek legislation to clarify and reduce the requirements for FFRDCs to access PROPIN.² Unfortunately, this change, if successful, would address PROPIN access for only a small percentage of personnel who support DoD and would leave in place the existing patchwork approach and lack of clarity about who is required to do what to access PROPIN.³ DoD will continue to encounter limits in support from nongovernment personnel until the matter is resolved. Perhaps just as important, DoD personnel will continue to work without clarity about uniform procedures and will likely continue the prevailing tendency of applying the PROPIN guidelines indiscriminately without attempting to parse the discrete pieces that actually merit restriction.

¹ As noted above, 10 U.S.C. 2320 specifically addresses technical data, so we are discussing only nontechnical data.

² 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 for an FFRDC to 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 CFR 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.

³ Legislative proposals such as the one summarized here would be included in the annual National Defense Authorization Act (NDAA). This specific proposal is intended to be part of the Fiscal Year 2017 NDAA, which would not take effect any earlier than October 1, 2016.

CUI Markings and Labels

Throughout the course of this study, the researchers found no evidence of a single authoritative source to turn to for questions regarding “how to share” data. A more robust, central program for CUI data labeling, access, and management (including monitoring and appeals) may facilitate smoother sharing and protection of CUI within DoD. DoD personnel should also receive up-front training on new CUI labeling procedures.

Given the lack of a central reference or authority for defining and establishing proper handling procedures for CUI, we recommend that a function and reference be established within OUSD(AT&L) for 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 for 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, OUSD(AT&L) would better understand how security policies are affecting their systems and whether a better balance between security and business cases is being achieved.

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

Third, a single individual should be designated with responsibility for implementing security strategy for a given information system and required system security classification guides. 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 who is familiar with the business case for a system to be more involved in the daily operations of that system and 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 and the use case 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. Required resources as part of policy design should be assessed, and the appropriate organization should provide at least some funding to address needed technical changes to the information systems.

DoD OGC Legal Opinion Dated February 1999

FEB-02-1999 11:52

F.002/003

OFFICE OF THE DEPUTY GENERAL COUNSEL
(ACQUISITION AND LOGISTICS)
DEPARTMENT OF DEFENSE
1 February 1999

MEMORANDUM FOR THE DIRECTOR, CONTRACTOR COST DATA REPORT PROJECT
OFFICE

Via: *[Signature]* DGC (A&L) *[Signature]* 1 Feb 99

This is in response to your 4 January 1999 request for a legal opinion concerning: (1) the adequacy of your procedures for disseminating contractor cost data report (CCDR) data; and (2) the applicability of those procedures to federally funded research and development centers (FFRDCs).

With respect to the first issue, since contractors generally consider and/or mark their cost data as proprietary, such information is normally required to be protected from public disclosure pursuant to various statutes, regulations, or policies, such as the Freedom of Information Act (FOIA), 18 U.S.C. § 1905 (a criminal statute concerning the disclosure of confidential information), the Procurement Integrity Act, the Competition in Contracting Act (CICA), and their implementing regulations and policies. Unauthorized release of such information to the public would result in harm to the originator or impair the Government's ability to obtain such information in the future. It also could result in criminal prosecution.

Exemption 4 of the FOIA applies to "trade secrets and commercial or financial information obtained from a person and privileged or confidential." Cost data provided by a contractor would generally be considered confidential commercial information requiring protection from public disclosure. In addition, FAR section 3.104, which implements the Procurement Integrity Act, provides that "contractor bid or proposal information" includes cost or pricing data and indirect costs and direct labor rates. Such information is required to be protected from disclosure to any person other than a person authorized, in accordance with agency procedures, to receive such information. To the extent any data listed on the CCDRs is also contractor bid or proposal information, it is subject to this restriction. Finally, to

FEB-02-1999 11:53

P.003000

preserve the integrity of the procurement process, contracting officers are required to maintain a high level of business security in accordance with FAR 5.401(a). To that end, contracting officers may make available maximum information to the public; exceptions include information that was received in confidence from an offeror or otherwise requiring protection under FOIA per FAR 5.401(b). Again, a contractor's cost data would generally fall within these exceptions.

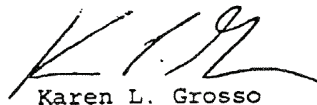
Against that background, we have no objection to the "modified" procedures you have set up to protect from disclosure such confidential commercial information. One recommendation with respect to your "Step 3," is to ensure that the non-disclosure agreement references the pertinent contract clause requiring the support contractor to protect the CCDC data and to return the data upon contract completion.

With respect to the second issue, FAR 35.017 provides:

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 facilities.

Based on this policy, it appears that your current practice of treating FFRDCs in the same manner as you do support contractors, but with "privileged access" to information available to Government personnel when such access is necessary for completion of assigned tasks, is reasonable.

Therefore, there is no objection to your procedures as outlined. If you have any questions regarding this matter or require additional information, please contact me at 692-9180.



Karen L. Grosso

Bibliography

Assad, Shay D., “Department of Defense Source Selection Procedures,” memorandum, Washington, D.C.: Director, Defense Procurement and Acquisition Policy, Acquisition, Technology and Logistics, Department of Defense, March 4, 2011.

Carter, Ashton B., “Federally Funded Research and Development Center (FFRDC) Management Plan and Associated ‘How-to-Guides,’” memorandum, Washington, D.C.: Acquisition, Technology and Logistics, Department of Defense, May 2, 2011.

Chairman of the Joint Chiefs of Staff Instruction 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*, Washington, D.C., February 9, 2011, current as of June 9, 2015.

CJCSI—see Chairman of the Joint Chiefs of Staff Instruction.

Controlled Unclassified Information Office, *What Is CIU? Answers to the Most Frequently Asked Questions*, Washington, D.C.: U.S. National Archives and Records Administration, 2011. As of March 29, 2014: <http://www.archives.gov/cui/documents/2011-what-is-cui-bifold-brochure.pdf>

Defense Acquisition Management Information Retrieval (DAMIR) information system, “Welcome to DAMIR WebHelp,” Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD(AT&L)) Acquisition Resources and Analysis (ARA) Directorate, undated. As of June 24, 2016: <https://ebiz.acq.osd.mil/DAMIR/WebHelp/index.html#!/Documents/welcometodamirwebhelp.htm>

Defense Acquisition University, “Acquisition Category (ACAT),” Acquipedia, modified on June 23, 2016. As of June 27, 2016: <https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=a896cb8a-92ad-41f1-b85a-dd1cb4abdc82>

DoD—see U.S. Department of Defense.

DoDD—see U.S. Department of Defense Directive.

DoDI—see U.S. Department of Defense Instruction.

DoDM—see U.S. Department of Defense Manual.

Earned Value Management, home page, undated. As of April 19, 2016: <http://www.acq.osd.mil/evm/>

Executive Office of the President, Office of Management and Budget, *Open Data Policy-Managing Information as an Asset*, Washington, D.C., May 9, 2013. As of January 29, 2016: <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf>

Executive Order 13556, *Controlled Unclassified Information*, Washington, D.C.: The White House, November 4, 2010.

GC Micro Corp. v. Def. Logistics Agency, 33 F.3d 1109 (9th Cir. 1994).

Grosso, Karen, “Memorandum for the Director, Contractor Cost Data Report Project Office,” Washington, D.C.: Office of the Deputy General Counsel (Acquisition and Logistics), Department of Defense, February 1, 1999.

Information Assurance Support Environment, “External Certification Authority Program (ECA),” last revised April 21, 2016. As of June 27, 2016: <http://iase.disa.mil/pki/eca/Pages/index.aspx>

Kendall, Frank, *Acquisition Information Repository Implementation Guidance*, September 25, 2012.

Legal Information Institute, “10 U.S. Code § 2320—Rights in Technical Data,” Cornell University Law School, undated. As of November 3, 2014:
<http://www.law.cornell.edu/uscode/text/10/2320>

Martin Marietta Corp. v. Dalton, 974 F. Supp. 37 (D.D.C. 1997).

Memorandum from the Assistant Secretary of Defense (Public Affairs), “Update: Interaction with OSD/PA on Release of Official Information,” September 2, 2010.

Memorandum from the Director, Defense Procurement and Acquisition Policy, “Department of Defense Source Selection Procedures,” March 4, 2011.

Nat’l Parks & Conservation Ass’n v. Morton, 498 F.2d 765, 770 (D.C. Cir. 1974).

National Science Foundation, “Master Government List of Federally Funded R&D Centers,” June 2015a. As of December 28, 2015:
<http://www.nsf.gov/statistics/ffrdclist/>

———, “Master Government List of Federally Funded R&D Centers: General Guidelines,” June 2015b. As of December 28, 2015:
<http://www.nsf.gov/statistics/ffrdclist/#gennotes>

Office of the U.S. Department of Defense Chief Information Office and Deputy Chief Management Officer, “Review of the Total Information Technology Operations Cost for the Pentagon Reservation and National Capital Region; Response to the Deputy Secretary of Defense (DSD) Memo Subject ‘Review of the Total Costs of the Pentagon Reservation Operations’ Dated October 2, 2014,” April 3, 2015. As of March 9, 2016:
<http://dodcio.defense.gov/Portals/0/Documents/BPSR/Consolidation%20of%20Pentagon%20Information%20Technology%20Operations.pdf>

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Acquisition Resources and Analysis (ARA) Directorate, “Deputy Director, Enterprise Information,” undated. As of June 27, 2016:
<http://www.acq.osd.mil/ara/office-ei.htm>

OUSD(AT&L)/ARA—see Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Acquisition Resources and Analysis (ARA) Directorate.

Riposo, Jessie, Megan McKernan, Jeffrey A. Drezner, Geoffrey McGovern, Daniel Tremblay, Jason Kumar and Jerry M. Sollinger, *Issues with Access to Acquisition Data and Information in the Department of Defense: Policy and Practice*, Santa Monica, Calif.: RAND Corporation, RR-880-OSD, 2015. As of December 24, 2015:
http://www.rand.org/pubs/research_reports/RR880.html

Treanor, William Michael, “Applicability of Trade Secrets Act to Intra-Governmental Exchange of Regulatory Information,” Memorandum, Office of Legal Counsel, U.S. Department of Justice, April 5, 1999.

U.S. Army, *Management: RAND Arroyo Center, Army Regulation 5-21*, Washington, D.C.: Headquarters, Department of the Army, May 25, 2015.

U.S. Code, Title 5, Section 552, *Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings*, January 16, 2014.

U.S. Code, Title 5, Section 3371, *Definitions*.

U.S. Code, Title 6, Section 985, *Information Sharing Relating to Supply Chain Security Cooperation*.

U.S. Code, Title 10, Section 122a, *Public Availability of Department of Defense Reports Required by Law*.

U.S. Code, Title 10, Section 129d, *Disclosure to Litigation Support Contractors*, January 16, 2014.

U.S. Code, Title 10, Section 2304, *Contracts: Competition Requirements*.

U.S. Code, Title 10, Section 2320, *Rights in Technical Data*.

U.S. Code, Title 10, Section 2321, *Validation of Proprietary Data Restrictions*.

U.S. Code, Title 10, Section 2367, *Use of Federally Funded Research and Development Centers*.

- U.S. Code, Title 18, Section 1905, *Disclosure of Confidential Information Generally*, January 16, 2014.
- U.S. Code, Title 28, Section 2679, *Exclusiveness of Remedy*.
- U.S. Code, Title 41, Section 2101, *Definitions*.
- U.S. Code, Title 41, Section 2102, *Prohibitions on Disclosing and Obtaining Procurement Information*.
- U.S. Code of Federal Regulations, Title 22, Section 120.10, *Technical Data*.
- U.S. Code of Federal Regulations, Title 48, Section 3.104-1, *Definitions*.
- U.S. Code of Federal Regulations, Title 48, Section 35.017, *Federally Funded Research and Development Centers*.
- U.S. Code of Federal Regulations, Title 48, Section 52.227-7013, *Rights in Technical Data*.
- U.S. Congress, 107th Cong., *E-Government Act of 2002*, Washington, D.C., H.R. 2458, Public Law 107-347, December 17, 2002.
- U.S. Department of Defense, "Department of Defense Information Assurance Certification and Accreditation Process," Personnel and Readiness Information Management, undated. As of March 9, 2016:
http://www.prim.osd.mil/Documents/DIACAP_Slick_Sheet.pdf
- U.S. Department of Defense Directive 5000.01, *The Defense Acquisition System*, Washington, D.C., May 12, 2003, current as of November 20, 2007.
- U.S. Department of Defense Directive 5105.53, *Director of Administration and Management (DA&M)*, Washington, D.C., February 26, 2008.
- U.S. Department of Defense Directive 5205.02, *DoD Operations Security (OPSEC) Program*, Washington, D.C., March 6, 2006.
- U.S. Department of Defense Directive 5400.07, *DoD Freedom of Information Act (FOIA) Program*, Washington, D.C., January 2, 2008.
- U.S. Department of Defense Directive 7045.14, *The Planning, Programming, Budgeting, and Execution (PPBE) Process*, Washington, D.C., January 25, 2013.
- U.S. Department of Defense Instruction 5000.02, *Operation of the Defense Acquisition System*, Washington, D.C., January 7, 2015.
- U.S. Department of Defense Instruction 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information*, Washington, D.C., October 9, 2008, incorporating change 1, June 13, 2011.
- U.S. Department of Defense Instruction 5230.24, *Distribution Statements on Technical Documents*, Washington, D.C., August 23, 2012.
- U.S. Department of Defense Instruction 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance*, Washington, D.C., July 14, 2015. As of June 27, 2016:
<http://www.dtic.mil/whs/directives/corres/pdf/540016p.pdf>
- U.S. Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, Washington, D.C., March 12, 2014.
- U.S. Department of Defense Instruction 8520.03, *Identity Authentication for Information Systems*, Washington, D.C., May 13, 2011.
- U.S. Department of Defense Manual 5200.01, Vol. 1, *DoD Information Security Program: Overview, Classification, and Declassification*, Washington, D.C., February 24, 2012.
- U.S. Department of Defense Manual 5200.01, Vol. 2, *DoD Information Security Program: Marking of Classified Information*, Washington, D.C., February 24, 2012.
- U.S. Department of Defense Manual 5200.01, Vol. 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)*, Washington, D.C., February 24, 2012.
- U.S. Department of Defense Manual 5205.02-M, *DoD Operations Security (OPSEC) Program Manual*, Washington, D.C., November 3, 2008.

U.S. Department of Defense Regulation 5400.7-R, *DoD Freedom of Information Act Program*, Washington, D.C., September 1998.

U.S. Department of Justice, *Department of Justice Guide to the Freedom of Information Act*, Washington, D.C., 2009. As of December 28, 2015:

<http://www.justice.gov/oip/doj-guide-freedom-information-act-0>

———, *U.S. Attorneys' Manual: Civil Resource Manual*, Washington, D.C., Chapter 33. Available as of December 30, 2015:

<http://www.justice.gov/usam/civil-resource-manual-33-immunity-government-officers-sued-individuals>

U.S. Federal Acquisition Regulation, Part 35.017, *Federally Funded Research and Development Centers*, September 3, 2015. As of January 28, 2016:

<http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/35.htm>

Acquisition data play a critical role in the management of the U.S. Department of Defense's (DoD's) portfolio of weapon systems. Identifying which unclassified but potentially sensitive data require protection as Controlled Unclassified Information (CUI) and how to properly protect them through the use of appropriate markings or labels can be difficult: Management and sharing of these data are subject to the interaction and interpretation of a number of laws, regulations, and policies. Therefore, the Office of the Secretary of Defense asked RAND to evaluate current CUI labeling procedures, practices, and security policies. The authors found that documentation on CUI labeling procedures is incomplete and unclear. To define and establish proper handling procedures for CUI, a function (additional responsibility for a currently existing office with experience using a large number of CUI labels in multiple roles) and reference (a central, authoritative online resource that references all relevant guidance on information management, handling, access, and release for acquisition data) should be established within the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.

Because the RAND Corporation operates three federally funded research and development centers (FFRDCs), the authors have an interest in FFRDC access to data. However, the authors believe that the results are valid independent of that interest. They also have firsthand experience with the struggles of DoD personnel managing data and access.



NATIONAL DEFENSE RESEARCH INSTITUTE

www.rand.org

\$24.00

ISBN-10 0-8330-9596-X
ISBN-13 978-0-8330-9596-1

