

# SAFEGUARDING MILITARY INFORMATION IN HISTORICAL STUDIES

A Handbook about Classified Information for  
Military Cultural Resource Managers



November 1, 2013

Completed under Contract Number: W9132T-12-2-0038



Legacy Project No. 12-516



# SAFEGUARDING MILITARY INFORMATION IN HISTORICAL STUDIES

A Handbook about Classified Information for Military Cultural  
Resource Managers

Prepared For  
Legacy Resource Management Program



Prepared By  
Van Citters: Historic Preservation, LLC



Authors:  
Karen Van Citters  
Brian M. Lione



## ACKNOWLEDGEMENTS

There are over 60 military Directives, Instructions, Manuals, and Regulations and a plethora of Executive Orders and other documents that apply to the protection of information and the subject of this handbook. All of these addressed the work of cultural resource managers and the requirements to protect military information—during this project, each time we found a document it would reference a number of other documents in a seemingly never-ending chain of references. The input and support of our subject matter experts were invaluable in aiding us to focus on the critical aspects for this handbook.

The authors would like to thank the following for their enthusiastic support, guidance, and patience throughout the process of developing this report. This group served as our subject matter experts, met with us multiple times, reviewed drafts of the document, and was generally available for questions and discussions.

For providing the information that generated the project and his continuing support throughout the work:

Michael Binder, Air Force Declassification Office

For subject matter expert meetings, continual email, phone, and text review support as the project developed:

Art Horn, Washington Headquarters Services, Defense Office of Prepublication & Security Review

Sean Carney, Deputy Under Secretary of the Navy for Plans, Policy, Oversight and Integration

Mark Myers, Office of the Under Secretary of Defense for Intelligence, Deputy Under Secretary of Defense (Intelligence & Security), Security Policy and Oversight

For providing input during subject matter expert meetings:

Daryl Haegley, ODUSD(I&E) Business Enterprise Integration, Energy & ICS Information Risk Management

William Manley, Naval Facilities Engineering Command, Headquarters

Jay Thomas, Naval History & Heritage Command

Devalee Gattison, Secretary of the Air Force, Public Affairs

Carolyn Taylor, Secretary of the Air Force, Public Affairs

CDR Jeremy Schaub, Office of the Deputy Assistant Secretary of the Navy for the Environment

Additional Document Reviewers:

Paul Green, Ph.D., Air Force Civil Engineer Center

Nancy Harrity, Navy Office of Information Requirements, Policy & Professional Development

Don Rochon and Virginia Bueno, Naval Facilities Engineering Command, Public Affairs

Hillori L. Schenker, Naval Facilities Engineering Command, Headquarters

David Werner, Asst. Director for Communications and Outreach, Naval Historic Heritage Command  
Greg Martin, NHHC, Histories and Archives  
Curtis Utz, NHHC

DoD Cultural Resource and Legacy Resource Management Program Support:  
Serena Bellew, Office of Secretary of Defense, Installations & Environment  
Cecilia Brothers, contractor support, Office of Secretary of Defense, Installations & Environment

NOTE: This report is intended to aid all DoD cultural resource professionals at all echelons, including installations, headquarters, regional support, and the Office of the Secretary of Defense. It is also intended for their contractors to ensure the contractors are aware of DoD policy and work toward safeguarding information as they develop their deliverables.

# TABLE OF CONTENTS

**ACKNOWLEDGEMENTS** ..... i

**ACRONYMS & ABBREVIATIONS** ..... viii

**INTRODUCTION**..... 1

    What Should be Safeguarded? ..... 1

    Typical CRM Challenges ..... 2

        Information Compilation ..... 2

        Derivative Classification ..... 3

        Retired Weapons Systems ..... 4

        Internet ..... 4

        Geospatial-Intelligence ..... 4

        Base Closures and Realignment 05 ..... 4

        Providing Access to Classified Sites / Areas ..... 5

        Oral Histories ..... 5

**ROLES & RESPONSIBILITIES** ..... 7

    Primary Project Participants ..... 7

    Other Important Classified Information Personnel ..... 13

**INFORMATION SECURITY POLICY**..... 15

    Federal Government Policy ..... 15

    Department of Defense Policy ..... 19

        DoD–Wide Documents ..... 20

            DoD Industrial Security ..... 20

            DoD Information Security Program ..... 20

            DoD Operations Security Program ..... 21

            Security and Policy Review of Information for Public Release ..... 21

            National Geospatial-Intelligence Agency ..... 22

    DoD Component Documents ..... 22

        U.S. Army ..... 22

        Department of Navy ..... 23

        U.S. Air Force ..... 25

    Summary ..... 26

**CLASSIFICATION PRIMER**..... 27

    National Security Information ..... 27

    Security Classification Guidance ..... 28

    Special Classified Information ..... 29

        Sensitive Compartmented Information ..... 29

        Special Access Programs ..... 29

    Classified Information ..... 30

        Restricted Data ..... 31

        Critical Nuclear Weapons Design Information ..... 31

        Formerly Restricted Data ..... 32

        Critical Technology ..... 32

Geospatial-Intelligence .....	33
Scientific and Technical Information .....	34
Controlled Unclassified Information .....	35
For Official Use Only .....	36
Freedom of Information Act .....	37
Access .....	38
Protection .....	38
Unclassified Controlled Nuclear Information .....	39
Access .....	39
Protection .....	39
Sensitive But Unclassified .....	40
Access .....	40
Protection .....	40
Geospatial-Intelligence (Unclassified) .....	40
Changes in Classification .....	41
Declassification .....	42
Duration of Classification .....	44
Declassification Date .....	44
Extending the Duration of Classification .....	45
Controlled Unclassified Information .....	45
Changing the Level of Classification .....	45
Unauthorized Disclosure .....	46
<b>PLANNING AND EXECUTING YOUR PROJECT .....</b>	<b>47</b>
Phase I: Conception and Initiation .....	49
Red Flag Issues .....	50
Information that May Require Higher Echelon Review .....	50
Sensitive Installation List .....	51
Critical Information List .....	52
Other Resources .....	52
Security Classification Guides .....	53
Military Critical Technologies List .....	54
International Traffic-in-Arms Regulations .....	54
Additional Information .....	55
Phase II: Definition and Planning .....	55
Contracting .....	56
In-House CRM Projects .....	57
Special Considerations for Historical Researchers .....	57
Incorporating Reviews into a Project .....	58
Phase III: Startup (Launch) .....	59
Contracting .....	59
In-House CRM Projects .....	60
Phase IV: Performance .....	60
Tracking the Project .....	60
Distribution Statement .....	61



Statement Requirements .....	61
Applying the Statement.....	64
<b>DEPARTMENT OF THE ARMY DOCUMENT REVIEW PRACTICES .....</b>	<b>65</b>
Purpose .....	65
Roles & Responsibilities .....	65
Public Affairs Program.....	66
Operational Security Program .....	69
Information Security Program.....	70
Geospatial-Intelligence.....	72
Process.....	72
Basic Review Times .....	73
Submittals.....	74
Contractor Submittals .....	74
Review Materials .....	75
Possible Outcomes .....	76
<b>DEPARTMENT OF THE NAVY DOCUMENT REVIEW PRACTICES .....</b>	<b>79</b>
Purpose .....	79
Roles & Responsibilities .....	79
Public Affairs Office .....	80
Public Affairs.....	80
Operational Security.....	81
Information Security Program.....	82
Geospatial-Intelligence.....	83
Process.....	83
Basic Review Times .....	86
Submittals.....	86
Possible Outcomes.....	87
<b>DEPARTMENT OF THE AIR FORCE DOCUMENT REVIEW PRACTICES .....</b>	<b>89</b>
Purpose .....	89
Roles & Responsibilities .....	89
Operational Security Program .....	89
Public Affairs and Information Security Program.....	90
Geospatial-Intelligence.....	91
Process.....	91
Operational Security Program .....	91
Public Affairs and Information Security .....	92
Basic Review Times .....	93
Submittals.....	94
Possible Outcomes.....	96
<b>RESOURCES .....</b>	<b>97</b>
Defense Office of Prepublication and Security Review.....	97
Department of the Army .....	97
Department of the Navy .....	97
Department of the Air Force .....	97
Defense Security Service .....	98

Defense Technical Information Center .....	98
Security Classification Guides.....	98
DoD Scientific and Technical Information Program.....	98
DTIC Customer Support.....	99
<b>DEFINITIONS .....</b>	<b>101</b>
<b>ANNOTATED BIBLIOGRAPHY .....</b>	<b>107</b>
Office of the Secretary of Defense .....	107
Industrial Security.....	107
Geospatial-Intelligence.....	107
Information Security.....	108
Operations Security .....	110
Public Affairs, Security and Policy Review Process, and Public Information.....	110
Department of the Army .....	112
Industrial Security.....	112
Information Security.....	112
Operations Security .....	112
Public Affairs / Security and Policy Review .....	112
Department of the Navy .....	113
Information and Personnel Security .....	113
Operations Security .....	113
Public Affairs / Security and Policy Review .....	114
United States Marine Corps .....	114
Information Security.....	114
Operations Security .....	114
Public Affairs / Security and Policy Review .....	114
Department of the Air Force .....	115
Industrial Security.....	115
Operations Security .....	115
Information Security.....	115
Public Affairs / Security and Policy Review .....	116
Information Security References, U.S. Federal Government.....	116
Executive Orders .....	116
Information Security Oversight Office .....	118
Information Security References, Non-Federal .....	118
<b>APPENDIX A: ACCESS TO CLASSIFIED INFORMATION .....</b>	<b>1</b>
Clearance Basics .....	2
Process to Obtain a Clearance.....	3
Application Results.....	5
Locating Past Results.....	6
Company Clearance .....	6
<b>APPENDIX B: STORING, HANDLING, AND TRANSMITTING INFORMATION .....</b>	<b>1</b>
Protecting Data During Document Development .....	2
Equipment.....	3
Communications.....	3

Storing Information .....	3
Handling Information .....	4
Data Spills.....	4
Destruction.....	5
Transmitting Information .....	5
Electronically.....	6
Secure Facsimile.....	6
Postal Service .....	6
Hand-carry.....	7
Conversation.....	7
Security Incidents.....	7
Consequences .....	8
<b>APPENDIX C: FORMS .....</b>	<b>1</b>
<b>APPENDIX D: NON-DISCLOSURE EXAMPLE FROM DD 254 ATTACHMENT .....</b>	<b>1</b>

**List of Figures**

Figure 1. Protected Information Organization Chart for U.S. Government and DoD / CRM.....	17
Figure 2. The Relationship between Collateral and Non-Collateral Designations .....	30
Figure 3. Section 106 and Safeguarding Information.....	48
Figure 4. U.S. Army, Public Affairs Program Organizational Chart.....	66
Figure 5. U.S. Army, CSM Organizational Chart.....	71
Figure 6. U.S. Army, Simplified CRM Security and Policy Review Chart .....	73
Figure 7. U.S. Navy, Public Affairs Office Organization Chart.....	80
Figure 8. U.S. Navy, CSM Organization Chart .....	82
Figure 9. U.S. Navy, Simplified CRM Security and Policy Review Chart .....	85
Figure 10. U.S. Air Force, Simplified CRM Security and Policy Review Chart .....	93

**List of Tables**

Table 1. Compilation of Information that Requires Protection .....	27
Table 2. CUI Markings .....	36
Table 3. Distribution Statement Types and Reasons .....	64

## ACRONYMS & ABBREVIATIONS

ACOM	Army Command
AFI	Air Force Instruction
AR	Army Regulation
ASM	activity security manager
BRAC	Base Closure and Realignment (1998 was Base Realignment and Closure)
CHINFO	U.S. Navy, Chief of Information
CI	Critical Information
CIL	Critical Information List
CMC	Commandant of the Marine Corps
CNO	Chief of Naval Operations
CNWDI	Critical Nuclear Weapon Design Information
CO	contracting officer [Navy, Air Force]
COR	contracting officer's representative
CRM	cultural resource manager
CSM	command security manager
CUI	controlled unclassified information
DD	Defense Department
DIRPA	Director of Public Affairs [Navy]
DoD	Department of Defense
DoD UCNI	Unclassified Controlled Nuclear Information (DOE)
DOE	Department of Energy
DON	Department of the Navy
DOPSR	Washington Headquarters Services, Defense Office of Prepublication & Security Review
DOS	Department of State
DTIC	Defense Technical Information Center
EO	Executive Order
FAR	Federal Acquisition Regulations
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FRD	Formerly Restricted Data
GEOINT	geospatial-intelligence
GIS	Geographic Information System
HQDA	Headquarters, Department of the Army
INFOSEC	information security
ITAR	International Traffic in Arms Regulations
IOSS	Interagency OPSEC Support Staff
ISOO	Information Security Oversight Office
ISP	Information Security Program
JCS	Joint Chiefs of Staff
KO	contracting officer [Army]

LES	Law Enforcement Sensitive Information
MCTL	Military Critical Technology List
NARA	National Archives and Records Administration
NGA	National Geospatial-Intelligence Agency
NISP	National Industrial Security Program
NSG	National System for Geospatial-Intelligence
NSI	National Security Information
OATSD(PA)	Office of the Assistant to the Secretary of Defense for Public Affairs
OCA	original classification authority
OCA	Office of the Chief of Public Affairs [Army]
ODUSD(I&E)	Office of the Deputy Under Secretary of Defense for Installations and Environment
OPSEC	operations security
OPR	office(s) of primary responsibility [Air Force]
OSD	Office of the Secretary of Defense
PA(O)	Public Affairs (Office; Officer)
POC	point of contact
RDT&E	research, development, test and evaluation
R&E	research and engineering
RD	Restricted Data
S&T	science and technology
SAF/PA	Secretary of the Air Force, Office of Public Affairs
SAP	special access programs
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCG	security classification guide
SECARMY	Secretary of the Army
SECNAV	Secretary of the Navy
SF	standard form
SNM	Special Nuclear Material
SME	subject matter expert
SP&R	Security and Policy Review [Air Force public affairs]
STINFO	Scientific and Technical Information
STIP	Scientific and Technical Information Program
UCNI	Unclassified Controlled Nuclear Information (DOE)
U.S.C.	United States Code
USD(I)	Under Secretary of Defense for Intelligence
USMC	United States Marine Corps
WHS	Washington Headquarters Services
WMD	weapons of mass destruction

Intentionally Blank

# INTRODUCTION

This handbook is designed to aid the Department of Defense (DoD) cultural resource manager (CRM) and their contractors in understanding the potential for the unauthorized disclosure of national security information that should be protected from public release and how to avoid such a disclosure on cultural resource projects. As a CRM it may seem that the content of your cultural resource reports is benign or that it couldn't possibly contain information that should be protected from public release (other than protected archaeological information); however, it is important to remember that if you haven't been trained in protecting national security information, you probably will not recognize military information that should be safeguarded when you see it. Something that seems minor to the cultural resource professional may in fact be a critical piece of information that could aid a U.S. adversary.

## **What Should be Safeguarded?**

Information that should be safeguarded is not just that which has been classified and is clearly marked as such. In developing a thorough historical study you may be: 1) providing specific details about military materiel or missions that are still considered operationally critical; 2) putting together a history using disparate unclassified sources that actually results in a document that should be classified or otherwise protected; 3) using information that you thought had been properly released, but was actually an unauthorized disclosure; or 4) using data that is not actually classified, but is considered controlled and should not be released. Each of the above scenarios can result in an unauthorized disclosure. You, as a CRM and Government employee or representative, have the ultimate responsibility for an unauthorized disclosure that results from the products that you release. If you knowingly, willingly, or negligently release information that you or your contractor produced, you can undergo sanctions or criminal prosecution.

Many cultural resource undertakings and reports have likely treaded into the above issues while the authors and project managers remained unaware that their project included such protected information. While this handbook is designed to assist CRMs in avoiding unauthorized disclosures, there are many security and policy review professionals in your organization and throughout the DoD who will aid you in developing your projects, support you, and ensure proper reviews prior to the public release of your CRM products. It is important for you to become familiar with who these people are, when you need to contact them, and how to ensure that your CRM information is properly reviewed prior to its release to the public.

U.S. security programs are designed to protect national security interests, while demonstrating a commitment to open government. The Government encourages sharing information. As a CRM you participate in consultation and public involvement efforts that require releasing information.

It is critical that you work with your security and policy review people to ensure that your work does not result in an unauthorized disclosure.

In order to translate DoD Directives, Instructions, Manuals, and other documents into language that is more reachable for the day-to-day work of a CRM, much of the information in this handbook has been paraphrased from the source documents. Throughout the text there are references to those documents; if you have any questions you should refer to those source documents and contact the professionals within your DoD Component and echelon to better understand the processes you should be using and the impacts on your projects and general work. Also be aware that from time to time the source documents are updated; be sure to check whether there are updates that may affect you.

### **Typical CRM Challenges**

Below are categories of typical challenges that face CRMs in the course of their work, which could result in the release of information that should be safeguarded.

### **Information Compilation**

As a CRM, you (or your contractors) will conduct archival research and prepare reports to develop determinations for eligibility of historic properties, historic structures reports, historic contexts, or other related documents to support historic preservation-related decisions. Combining detailed historical information to prepare these documents can be problematic and actually lead to potential classified and / or sensitive information handling requirements. The combining of information is known as compilation (as defined in DoD Manual 5200.01); however, your ASM/CSM will most likely refer to it as “aggregation.”<sup>1</sup> Compilation occurs when information that is based on a number of unclassified or previously released sources is put together and results in a document that should be classified or treated as CUI. So, even though your contract may not be considered to include classified information and you are not anticipating any protected information issues, in the course of the work to develop a thorough history such issues may arise through the amassing of research data.

A source document that a historian may find in an archive may be unclassified because it only tells a piece of the history or it does not provide specific, detailed data on military capabilities or missions. In order to understand the larger story or mission, historians will research numerous documents and put the picture together, which is required in order to understand eligibility or to develop a nuanced history. However, it is that assembly of history that can result in aggregation. Internet sources, libraries, archives, and previously cleared information can all be aggregated to create a product that includes information that should be protected. When you or your contractor are putting information together, you may not realize the net result should be classified or

---

<sup>1</sup> Department of Defense. DoD Manual, 5200.01, Volume I, *DoD Information Security Program: Overview, Classification, and Declassification*, Enclosure 4, pp. 41-43.



considered CUI, which is one of the reasons why projects that are not considered to include classified information also require a security and policy review.

Aggregation does not automatically occur when conducting a research project, developing historical documentation, or compiling multiple sources of information. Compiled information may be considered classified “only if its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security.”<sup>2</sup> It is also an issue if the aggregation falls into one of more of eight specific categories described in EO 13526—some of the categories that are likely to directly apply to CRM research and reporting efforts include:<sup>3</sup>

- Military plans, weapon systems, or operations
- Scientific, technological, or economic matters relating to national security
- U.S. Government programs for safeguarding nuclear materials or facilities
- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security
- The development, production, or use of weapons of mass destruction

In order to ensure that aggregation is not occurring or has not occurred, you—as the representative of the program that created the compilation—will need to facilitate a security and policy review of the products your program generates. To accomplish this, you will need to follow the process, depending on your DoD Component, as defined in process sections of this report. In general, you should make co-workers and contractors working on cultural resource projects aware of the potential for the aggregation of information. You should also alert your ASM/CSM immediately if you have a concern that a project is resulting in the compilation of information.

### **Derivative Classification**

Derivative classification applies when classified information has been incorporated, paraphrased, restated, or generated in a new form. If classified information is used in this manner, the newly developed material must be marked to be consistent with the OCA source information (the same level and declassification data will apply). The duplication or reproduction of existing classified information is not considered derivative classification. Duplicated materials require protection as noted in the Classification Primer section of this handbook.

If you, or your contractor, are creating derivatively classified information, you / they must mark the draft material and keep records of the sources that were used. These markings and source

---

<sup>2</sup> Ibid., p. 33.

<sup>3</sup> Executive Order 13526, “Classified National Security Information,” Subsection 1.4: *Classification Categories*, December 29, 2009. Other categories may apply; consult the full list in this EO as well as the requirements in DoD Manual, 5200.01, Volume 1.

materials will be used by a derivative classifier to ensure proper classification of the final product.<sup>4</sup>

### **Retired Weapons Systems**

Often in CRM, because you are developing military history, you work with weapons systems that are no longer in DoD service; however, these systems may still be in use by U.S. allies or they may be associated with information that would be of use to U.S. adversaries. If the system is still in use by an ally, it is likely that associated information about the system remains classified. Also, out-of-date systems are generally more easily replicated—there are certain historical systems that the U.S. would not want revealed because adversaries could use the information to develop weapons systems they otherwise would not have. If you or your contractors are working with a retired weapons system, it is important to determine whether there is an SCG that applies, within or outside your DoD Component. For example you could be working with a retired Air Force missile system, but the applicable SCG could be a Navy guide. If there is an applicable guide, refer to that guide—it will be specific on what you can and cannot say about the outdated system.

### **Internet**

We all know that information on the Internet may not be entirely accurate; while .gov sites are generally better than most, the information gathered from them will still require scrutiny. It is also important to keep in mind that if you find a DoD historical document or recent report that the upload of this information to the Internet may have been an unauthorized disclosure. Just because you found it on the Internet does not mean it went through a proper security and policy review prior to being put there—this can be particularly true for documents discussing retired weapons systems. This is unfortunate, but because of the ease of uploading to the Internet, it does occur. Using data obtained from the Internet is another reason it is required to have a security and policy review of the resulting documents prior to public release.

### **Geospatial-Intelligence**

Your DoD Component defines its own process for review of GEOINT for public release. If your map shows information that is generally available in sources such as Google Earth, it is probably okay to include in your report; however, if you add labels and other data to the map, you could be aggregating information that will require a review.

### **Base Closures and Realignment 05**

The Internet and other digital tools that were not available in previous Base Closure and Realignment (BRAC) rounds were critical in helping the DoD meet its environmental

---

<sup>4</sup> DoD Manual, 5200.01, Volume I, *DoD Information Security Program: Overview, Classification, and Declassification*, p. 39-40.

responsibilities during BRAC05. While these technologies supported the coordination of information, public involvement, and other aspects, because they had never been used before, they could have facilitated the release of sensitive information. Those that published the information did not recognize this possibility. If you or your contractor is using sources from BRAC05, it is possible that the information was minimally reviewed before release. Your product should undergo a proper review to ensure you have not inadvertently included any sensitive information.

### **Providing Access to Classified Sites / Areas**

From time to time, you may need to provide access to a classified area or site for consulting parties or a contractor. It is likely that the group or tenant at that location may tell you that you cannot obtain access. While the location may be restricted, this does not mean that it cannot be “sanitized” for a visit for officials, researchers, or others who require access to support you in your duties as CRM. In some cases, a site can be sanitized immediately and in others you will have to work with the group in advance of a visit and may be required to visit at a specific, arranged time. If the people at the site are reluctant to provide such access, contact your ASM/CSM, OPSEC Manager, and / or PA. These security and policy professionals can aid you in obtaining the necessary access so you may complete your work.

### **Oral Histories**

When conducting oral histories, your interviewee may be reluctant to share information that was classified when he was in still in the military or, conversely, he may think that the information he knows probably is not classified anymore. In either case, you or your contractor will have the need to collect accurate information and protect it if necessary. This can become a “Catch 22” if you and / or your contractor are not cleared—it is best to work with the ASM/CSM at your echelon to identify whether potential issues may arise and develop a plan on what to do if it should.

Prior to any interviews, it will be important to work with your ASM/CSM and OPSEC personnel to determine whether there is an SCG that applies to the topic or whether you have the potential to be collecting information that should be protected. Obtain documentation of this to share with your interviewee(s) and let them know in advance of the interview if the materiel, mission, or program they will be discussing has been declassified. If it has not been declassified, be sure to develop a plan for the discussion that will collect the data you require without compromising classified information.

If during an interview, it seems like your interviewee provided information that is classified, you should contact your ASM/CSM and / or OPSEC personnel to ensure the proper protocols are put into place to protect the information. It is possible that you might not know whether such

information has been provided via an oral history interview, so it is good policy, if possible, to have all your interviews vetted by your ASM/CSM and OPSEC personnel.

If you only remember one thing after reading this handbook, remember this:

**ALL DoD INFORMATION WHETHER UNCLASSIFIED, CUI OR CLASSIFIED MUST BE REVIEWED AND APPROVED FOR RELEASE through standard DoD Component processes before it is provided to the public!**

## ROLES & RESPONSIBILITIES

“All personnel of the Department of Defense are personally and individually responsible for properly protecting classified information and [controlled unclassified information] under their custody and control. All officials within the Department of Defense who hold command, management, or supervisory positions have specific, non-delegable responsibility for the quality and effectiveness of implementation and management of the information security program within their areas of responsibility.”

DoD Manual 5200.01, Enclosure 3

All personnel in the DoD have the responsibility to protect classified and controlled unclassified information (CUI)<sup>5</sup>; however, CRMs should pay particular attention to this because in writing military history and documenting our military cultural heritage there is the potential to release information that should be protected. Whether your project is originally considered classified or unclassified, the deliverables or products must be reviewed and approved for release through standard DoD Component processes before it can be released to the public.<sup>6</sup> Fortunately, there are many DoD personnel who are trained in protecting information and will aid you in the process. There is protocol that identifies the DoD project participants who will have important roles on your project. Below are descriptions of the primary personnel who you should be consulting in the course of your cultural resource work.

### **Primary Project Participants**

The primary participants in a cultural resource project will include the CRM, Contracting Officer<sup>7</sup>, public affairs officers (PAO), operations and information security (INFOSEC) managers at varying echelons, Defense Office of Prepublication and Security Review (DOPSR), original classification authorities (OCA), and potential outside agencies. In addition, there may be levels of internal review or other processes that are required at your echelon—you will need to make sure you are familiar with your local processes and that you incorporate them into your project management. You may also want to include the Program Manager / Project Action Officer or other such subject matter expert on your project, as they can provide input and review of your work.

---

<sup>5</sup> CUI has not yet been formally adopted; however, the categories of information that comprise CUI are currently recognized and the text about them will apply to your daily work. In the future, the term CUI will apply.

<sup>6</sup> In accordance with DoD Directive, Number 5230.09, *Clearance of DoD Information for Public Release*, August 22, 2008; DoD Directive 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, November 6, 1984; and DoD Instruction 5230.27, *Presentation of DoD-Related Scientific and Technical Papers at Meetings*, October 6, 1987.

<sup>7</sup> Acronyms: Air Force uses CO, Army uses KO, and Navy does not have an official acronym. Contracting Officer is spelled in full throughout the document for consistency and clarity.

**Cultural Resource Manager** [CRM] oversees the prehistoric and historic resources at their echelon. They aid their organization in meeting the requirements of the National Historic Preservation Act of 1966, DoD Directives, Instruction, and other guidance with regard to cultural resources. They are involved in understanding, preserving, and aiding their component in regulatory compliance when there are undertakings that affect cultural resources. CRMs produce and oversee work that results in reports available to the public—these deliverables in the past may have inadvertently released data that should have been protected.

CRMs have the responsibility to ensure that their projects have been properly reviewed by public affairs (PA) and their security managers. If you, as a CRM, fail to have the documents / deliverables produced by your office undergo a security review, you could be disclosing protected information. If this is done knowingly, willfully, or negligently, it could result in sanctions<sup>8</sup> or criminal prosecution.<sup>9</sup>

CRMs should be prepared to explain themselves and their programs to INFOSEC, OPSEC and PA personnel, many or all of whom may be unfamiliar with the job's requirements. These individuals may not have had previous experience with CRM programs, and may not understand the difference between CRM and the functions of the historian community. CRMs should be sure to highlight how their work fits into the larger environmental compliance framework, especially for projects that have legal drivers, required consultation requirements, and deadlines (such as Section 106). Other projects that lack an obvious legal requirement, but support program efficient and mission readiness, should also be clearly explained. These projects might include Section 110 surveys, ICRMP updates, or program alternative development), among others. CRMs may also need to explain their work to installation / activity historians or history office personnel for similar reasons.

A suggested approach for the CRM might include 1) how to describe the CRM mission and where it comes from, 2) the program contexts of CRM standard products (Section 106 letters and consultation, MOAs / PAs and agreement documents, ICRMPs, others), and 3) the ways in which CRM products are unusual from an INFOSEC / OPSEC perspective, and how those unusual features have been successfully solved. Taken together, these few suggestions comprise an additional tool to help the familiarization dialog go well from the start.

**Contracting Officers** have the authority to enter into, administer, or terminate contracts and make related determinations and findings. The Contracting Officer may bind the Government only to the extent of the authority delegated to them in writing; information on the limits of a

---

<sup>8</sup> Sanctions include warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, or denial of access to classified information.

<sup>9</sup> DoD Manual, Number 5200.01, Volume I, *DoD Information Security Program: Overview, Classification, and Declassification*, February 24, 2012, Enclosure 3, p. 32.

Contracting Officer authority is readily available to the public and agency personnel. No contract will be entered into unless the Contracting Officer ensures that all requirements of law, Executive Orders (EO), regulations, and all other applicable procedures, including clearances and approvals, have been met.

In addition, the Contracting Officers are responsible for ensuring performance of all necessary actions for effective contracting, ensuring compliance with the terms of the contract, and **safeguarding the interests of the United States** in its contractual relationships. In order to perform these responsibilities, Contracting Officers are allowed wide latitude to exercise business judgment. Basically they are required to:

1. Ensure that the requirements to enter into a contract (as noted above) have been met and that sufficient funds are available for obligation.
2. Ensure that contractors receive impartial, fair, and equitable treatment.
3. Request and consider the advice of specialists in audit, law, engineering, transportation, and other fields, as appropriate.<sup>10</sup>

The Contracting Officer has an important role in ensuring that CRM projects are properly reviewed before being released to the public; because Contracting Officers are warranted and part of their mandate is the safeguard the interests of the U.S., ultimately your Contracting Officer will become the hub of the review process for a contracted project. As with the technical content of a contracted project, it will be important to also provide your Contracting Officer with information about the potential for working with information that will require in-depth reviews or even a classified data contract (which requires different procedures than a contract that does not use classified data).

**Public Affairs Officer [PAO]** for any given organization / echelon provides review of documents to ensure the dissemination is consistent with DoD protocols and can be approved for release. In general a PAO at a specific echelon will analyze the military mission, unit policies, and relationship with the population of local communities to determine requirements for communication. The PAO develops and maintains a working relationship with media representatives, as well as with representatives of civilian organizations, governmental agencies, Reserve and active duty units, and other public organizations. The PAO is also responsible to develop plans and operational procedures for communication about aircraft and missile accidents, natural disasters, environmental incidents, and other spot news events concerning military activities. Ultimately, the PAO plans communication programs to ensure military and civilian members are informed about current issues and policies at their echelon.

---

<sup>10</sup> General Services Administration. DoD, National Aeronautics and Space Administration. *Federal Acquisition Regulation, Volume I, Parts 1-51*, March 2005, Title 48—Federal Acquisition Regulations System, Subpart 1.6, 1.602-2 Responsibilities, p. 1.6-1.

Your PAO will review CRM deliverables to ensure they are within the protocols of the PA mission. The PAO will assess your document given the plans, operational procedures, and communication program for your echelon and identify whether your document should move to a higher echelon—*typically the PAO will not identify whether there is a particular security management issue.*

**Activity (or Command) Security Manager** [ASM/CSM] implements the information security program (ISP) for his/her echelon in accordance with DoD Manual 5200.01 and the respective DoD Component senior agency official via directives, instruction, manuals, and other policy.

*TIP: Know the players, their roles, how and when to contact them. Build relationships so you and the military information professionals can support each other as the project develops. This will ensure your project progresses without significant delays.*

The ASM/CSM is responsible for conducting a security and policy review of information slated for public release. A security and policy review, or pre-publication review, is the process by which information proposed for public release is examined to ensure compliance with established national and DoD policies, and to determine that it contains no classified, CUI, or export controlled information—basically that it will not jeopardize ongoing or future military operations. This individual is specifically designated in writing and is

responsible for the ISP at the organization at which he / she works. The ASM/CSM guarantees that classified information<sup>11</sup> and CUI are properly handled by ensuring information is appropriately identified, marked, stored, disseminated, disposed of, and accounted for. If there are security incidents, they provide guidance on handling such incidents to minimize damage and ensure that appropriate corrective action is taken. The ASM/CSM may also be assigned responsibilities in other security disciplines such as personnel and physical security, etc.

Your ASM/CSM will review CRM products to ensure that there are no security issues associated with the content. They will also be assessing whether the product should move to a higher echelon for review, whether an outside agency should review, and / or whether the OCA (see below) of the content should be involved in the review.

**Operations Security Manager** [OPSEC Manager] implements the operations security (OPSEC) program for his / her organization in accordance with DoD Manual 5205.02, *Operations Security Program Manual*, and the respective DoD Component senior agency official. An OPSEC Program involves the design, implementation, and maintenance an evaluative process of an activity or unit to determine whether there are sufficient countermeasures to protect Critical Information (CI). CI includes details about U.S. military actions that could be beneficial to U.S.

<sup>11</sup> Except SCI which is the responsibility of the Special Security Officer appointed by the senior intelligence official; your ASM/CSM will let you know whether your project includes SCI.



adversaries if they were interpreted or pieced together in a way that would pose an unacceptable risk to U.S. operations.<sup>12</sup>

In coordination with their commanders, OPSEC Managers create and maintain Critical Information Lists (CILs) that are specific to their organization and contain elements of information deemed critical in order to protect tactical and strategic operations. OPSEC Managers also implement the “OPSEC process,” which generally involves analyzing friendly programs, projects, and activities to make sure they are not inadvertently sharing important information with the enemy—which means they may be looking at your CRM program.

OPSEC Managers will conduct an OPSEC Review of any information that you plan to release to the public, which includes CRM reports, surveys, studies, and other relevant documents. During the review, OPSEC Managers will compare your documents against CILs to ensure no release of information that could allow U.S. adversaries to compromise military operations; however, they will not be reviewing for historic CILs which may include information an OCA would consider restricting. This is why the OPSEC Manager will also work closely with your PAO, ASM/CSM, website administrators, and other officials designated by the DoD Component who also share responsibility for the release of information. Commanders and directors within your organization are responsible to identify whether there is a valid mission need to disseminate the information you are planning on sharing and to ensure that proper review procedures are implemented.<sup>13</sup>

**Original Classification Authority [OCA]** is the official authorized in writing, either by the President, an agency head, or other official designated by the President “to classify information originally” or “to make an original classification decision.” The OCA is the person who determines whether certain information should be classified, at what level, and when it should be declassified; it is also likely that this person will develop an associated security classification guide (SCG) for the materiel or program that was classified.

If your ASM/CSM has concerns over whether specific subject matter in your CRM project requires additional review, they will transfer your project to the OCA or a derivative classifier/declassifier for an additional review to ensure protected data is not released. It is likely that you, the CRM, would not communicate directly with an OCA; however, you may have conducted research into the SCGs that apply to your subject matter and may be aware of the potential for an OCA review.

**Washington Headquarters Services/Defense Office of Prepublication and Security Review [DOPSR]** conducts the security and policy review for clearance of official DoD information that

---

<sup>12</sup> Under Secretary of Defense for Intelligence. DoD Directive 5205.02E, *DoD Operations Security Program*, Part II, Definitions, June 20, 2012, p. 11.

<sup>13</sup> Under Secretary of Defense for Intelligence. DoD Manual 5205.02-M, *DoD Operations Security Program Manual*, Enclosure 5, November 3, 2008, p. 30.

is proposed for official public release by the DoD and its employees, both military and civilian. This review provides accurate and unclassified information to the public, the Congress, and the news media to help them understand defense strategy and national security issues. Official DoD information that is prepared by or for DoD personnel and is proposed for official public release is required to be submitted for a DOPSR security and policy review if the information:

- Originates or is proposed for release in the National Capital Region
- Is or has the potential to become an item of national or international interest
- Affects national security policy, foreign relations, or on-going negotiations
- Concerns a topic of controversy among DoD Components or with other Federal agencies
- Is presented by a DoD employee, who by virtue of rank, position, or expertise would be considered an official DoD spokesperson
- Contains technical data, including data developed under contract or independently developed and potentially controlled by the International Traffic in Arms Regulations (ITAR)—which may be militarily critical and subject to limited distribution, but on which a distribution determination has not been made
- Bears on any of the following subjects:
  - New weapon or weapons systems, or significant modifications or improvements to existing weapons or weapons systems, equipment or techniques
  - Military operations, significant exercises, and OPSEC of national or international significance
  - The President and/or Secretary of Defense; Command, Control, Communications, Computers and Intelligence; Information Operations; Weapons of Mass Destruction (WMD), except those covered by the Atomic Energy Act; Improvised Explosive Devices; and computer security
  - Military activities or application in space; nuclear weapons, including nuclear weapons effects research; chemical warfare and defensive biological warfare; initial fixed weapons basing; and arms control treaty implementation<sup>14</sup>

If your CRM product contains any of the above categories of information, it will require a DOPSR security and policy review. The ASM/CSM at your echelon will review your document first and then transmit to the appropriate DoD Component and / or DOPSR. Procedures and the timing of this higher level of review are located in Document Review Practices sections of this document.

---

<sup>14</sup> Compiled from: Department of Defense. DoD Manual, Number 5200.01, Volume I, *DoD Information Security Program: Overview, Classification, and Declassification*, February 24, 2012 and information available on the DOPSR website <http://www.dtic.mil/whs/esd/osr/> under the Washington Headquarters Services tab.

## **Other Important Classified Information Personnel**

**National Geospatial-Intelligence Agency [NGA]** is responsible for formulating, coordinating, and implementing policy for the classification, control, disclosure, and release of accurate geospatial-intelligence (GEOINT). The organization also has the ultimate review over geographic information system (GIS) data and other mapping that may be released to the public during the course of your CRM work. Your DoD Component has policies with regard to the development and maintenance of GEOINT and while within your DoD Component your PA, ASM/CSM, or OPSEC Manager may provide review and input on your use of GIS or other mapping data in your products. They may also refer your project to NGA for review to ensure classified or otherwise protected GEOINT does not become an unauthorized disclosure.

There are many other security professionals and groups who are engaged in protecting national security information (NSI), such as Top Secret Control Officer communication security, North Atlantic Treaty Organization, Control Point Officer; Special Security Officer; Special Access Programs (SAP); Information Systems Security Officials and Information Assurance Managers; and Counterintelligence. These are all important personnel with regard to safeguarding military information; however, it is less likely that a CRM would be in communication with one of these custodians or officers regarding the content of a cultural resource report. If one of them should be involved in your project, refer to DoD Manual 5200.01, Volume I, Enclosure 3 to ascertain their role and duties so you can better understand the effect on your project and when you should be interacting with them.

Intentionally Blank

# INFORMATION SECURITY POLICY

## **Federal Government Policy**

At the Federal Government level, Federal policy for INFOSEC is derived from EOs and laws. EOs are often amended or entirely replaced with a new EO under a new administration, so it is important to reference the most recent set of policies. These orders set the overall tone for the handling of information and include attitudes towards classification and declassification. Under authority from EO 13526 and EO 12829, the Information Security Oversight Office (ISOO) is responsible to the President for policy and oversight of the Government-wide security classification system and the National Industrial Security Program (NISP). ISOO is a component of the National Archives and Records Administration (NARA) and receives policy and program guidance from the National Security Council (NSC). ISOO has three components: the Classification Management Staff, the Operations Staff, and the Controlled Unclassified Information Office.<sup>15</sup>

In the DoD there is a connection to ISOO through the Under Secretary of Defense for Intelligence (USD(I)), who is ultimately responsible for security and policy reviews at all echelons. With regard to cultural resource work, other DoD organizations include the Office of the Assistant to the Secretary of Defense for Public Affairs (OATSD(PA)) and the Office of the Deputy Under Secretary of Defense for Installations and Environment (ODUSD(I&E)). OATSD(PA) is responsible for the PA duties and staff at all echelons. The Federal Preservation Officer for the DoD resides within ODUSD(I&E) and has the responsibility for cultural resource duties and staff at all echelons.

*TIP: Become familiar with military information policies to ensure your work does not result in an unauthorized disclosure. This document synthesizes the processes for you, but you may also want to consult the source documents during the course of your work.*

DOPSR works directly with DoD Component Head PA and ASM/CSMs, but can also provide general information to DoD personnel at any echelon that may have a security and policy review question. As a CRM, whatever echelon you may be at, there will be PA and ASM/CSMs available to aid you in ensuring your projects do not release protected information to the public. Figure 1 shows an overview of the different government organizations that are involved in this process. Later in the handbook there are more detailed charts that show the DoD personnel you may be working with on a specific project.

<sup>15</sup> More information on the ISOO and its functions can be found at <http://www.archives.gov/isoo/>.

Intentionally Blank

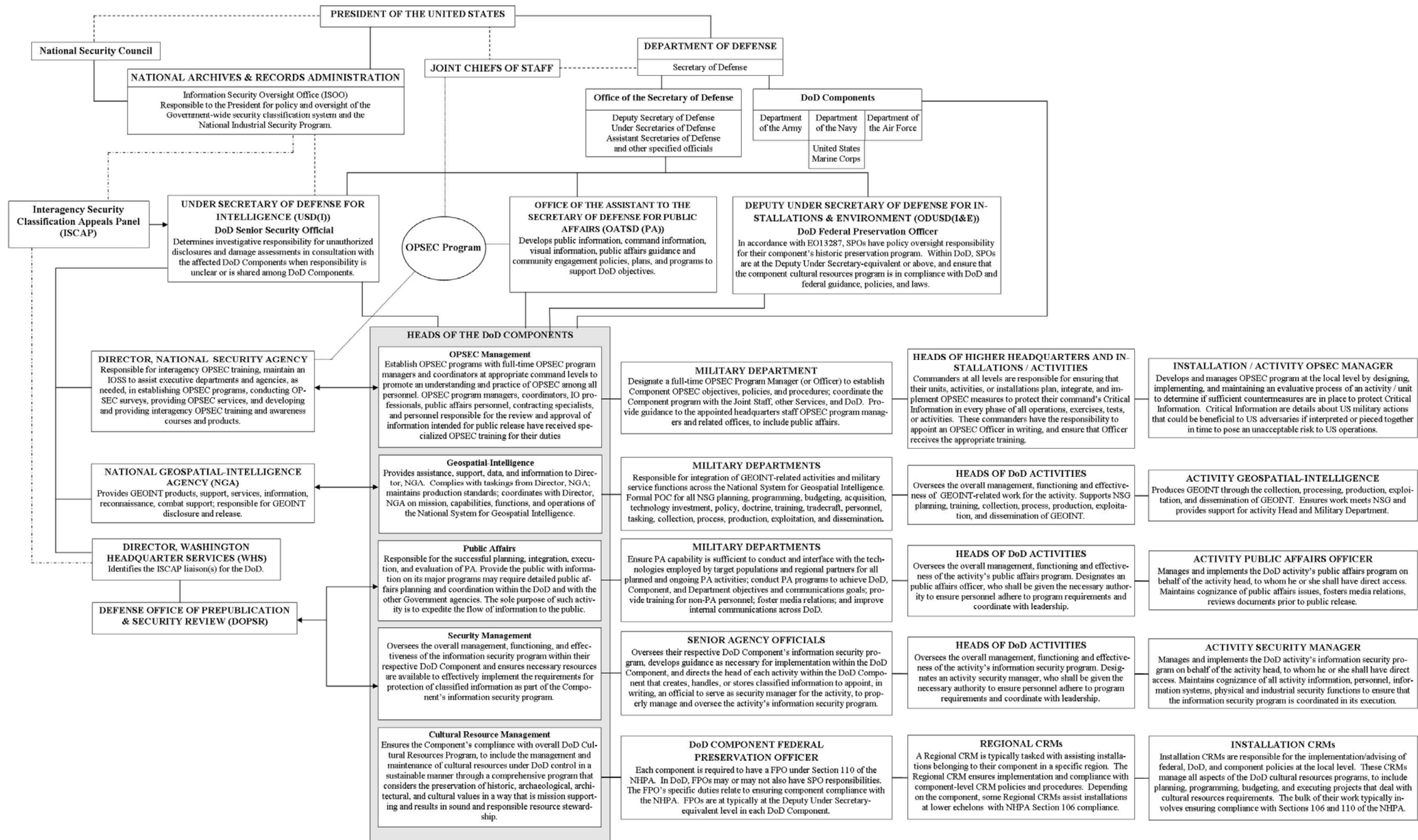


Figure 1. Protected Information Organization Chart for U.S. Government and DoD / CRM

Intentionally Blank



The following orders and regulations currently govern INFOSEC practices in the U.S. and for the Federal Government:

Executive Order 12829 (1993)—*National Industrial Security Program*

This order establishes a program to safeguard Federal Government classified information that is released to non-government organizations, such as contractors, licensees, and grantees in a manner that is equivalent to the protections required for the Government.<sup>16</sup>

Executive Order 12968 (1995)—*Access to Classified Information*

This order establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

Executive Order 13526 (2009)—*Classified National Security Information*

This order prescribes a uniform system for classifying, safeguarding, and declassifying NSI, including information relating to defense against transnational terrorism.

Executive Order 13549 (2010)—*Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*

This order applies uniform implementation standards to EO 12829, EO 12968, EO 13526, and EO 13467<sup>17</sup> to ensure consistent application between the requirements that govern access to and safeguard of classified material.

Executive Order 13556 (2010)—*Controlled Unclassified Information*

This order establishes an open and uniform program for managing information that is not classified, but requires safeguarding or dissemination controls.

International Traffic in Arms Regulations (ITAR; 22 CFR Parts 120-130; 1 April 2012)

This set of regulations promulgated by the Department of State (DOS) controls the import and export of articles and materials related to defense purposes. 22 CFR Part 125, *Licenses for the Export of Technical Data and Classified Defense Articles* specifically discusses the restrictions and requirements concerning export of unclassified and classified data.

## **Department of Defense Policy**

There are numerous DoD Directives, Instructions, and Manuals that respond to the Federal Government policies that relate to the proper treatment and handling of information. These are general policies which are expanded upon in greater detail by each DoD Component, whose policies are also noted in this document. Broadly, these policies address the requirements for INFOSEC, which is defined as the system of policies, procedures, and requirements to protect

<sup>16</sup> A related EO, Executive Order 12885 (1993), extended the time allotted to produce a Manual for EO 12829.

<sup>17</sup> Applies to the Executive Branch.



**DoD**

***Industrial Security***

- DoD Directive 5220.6
- DoD Instruction 5220.22
- DoD Manual 5220.22-M
- DoD Regulation 5220.22-R

***Information Security***

- DoD Directive 5205.7
- DoD Instruction 5200.01
- DoD Instruction 5205.11
- DoD Instruction 5210.02
- DoD Instruction 5210.83
- DoD Manual 5200.01 (4 vol)
- DoD Manual 5200.45
- DD Form 254

***OPSEC***

- DoD Directive 5205.05E
- DoD Manual 5205.02

***Public Affairs, Security and Policy Review Process, and Public Information***

- DoD Instruction 3200.12
- DoD Instruction 5122.05
- DoD Directive 5210.50
- DoD Directive 5230.09
- DoD Instruction 5230.29
- DoD Directive 5230.24
- DoD Directive 5230.25
- DoD Directive 5400.7
- DoD Regulation 5400.7-R
- DoD Instruction 5400.13
- DoD Instruction 8550.01
- DD Form 1910

***GEOINT***

- DoD Directive 5105.60
- DoD Instruction 5030.59
- DoD Instruction 3115.15
- JCS Instruction 3901.01C

information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security.<sup>18</sup> INFOSEC applies to unclassified and classified information alike.

In addition to INFOSEC requirements, you should be familiar with OPSEC requirements. In general, OPSEC is concerned with CI that U.S. adversaries need in order for them to succeed in their mission. Often, CI can be unclassified information that is seemingly innocuous, but still important to properly handle and protect through the established review processes for INFOSEC, OPSEC, and PA. Only through these reviews can you ensure that the work you are sharing beyond the DoD fence line does not compromise national security, mission capabilities, or readiness. Strict adherence to these review requirements will aid in mission success by preventing inadvertent compromise of CUI or classified activities, capabilities, or intentions at the tactical, operational and strategic levels.

**DoD–Wide Documents**

***DoD Industrial Security***

DoD Directive 5220.6 provides the policies, responsibilities, and procedures for the Defense Industrial Personnel Security Clearance Review Program. It is the baseline document for obtaining a security clearance for access to Confidential, Secret, or Top Secret information. It also includes procedures to safeguard information within industry that supports the Government. DoD Manual 5220.22-M and DoD Regulation 5220.22-R includes the detail on how to carry out the associated industrial security EOs and Directive 5220.6.

***DoD Information Security Program***

DoD Manual 5200.01 consists of four volumes that contain implementation policies for roles, responsibilities, and requirements of DoD INFOSEC. As per this manual, and the related DoD Directives and Instructions that drive it, it is DoD policy to identify and protect NSI and CUI in accordance with national level policy issuances; promote information sharing, facilitate judicious use of resources, and simplify management

<sup>18</sup> DoD Manual, 5200.01, Volume I, *DoD Information Security Program: Overview, Classification, and Declassification*, p. 80.

through implementation of uniform and standardized processes; and classify and declassify NSI as required by federal mandates. The volumes are collectively known as the *DoD Information Security Program* and they include:

*Volume 1: Overview, Classification, and Declassification* (updated 2012). Describes classification and declassification policies for the designation, marking, protection, and dissemination of classified information.

*Volume 2: Marking of Classified Information* (updated 2013). Provides guidance for using the correct classification markings for documents and other DoD products.

*Volume 3: Protection of Classified Information* (updated 2012). Provides guidance for safeguarding, storage, destruction, transmission, and transportation of classified information; identifies security education and training requirements and processes for handling of security violations and compromise of classified information; addresses information technology issues of which the security manager must be aware; and incorporates command, control, and communication information.

*Volume 4: Controlled Unclassified Information* (updated 2012). Provides guidance for the identification and protection of CUI.

### ***DoD Operations Security Program***

It is DoD policy to establish and maintain OPSEC programs to ensure national security-related missions and functions are protected. DoD Manual 5205.02 defines DoD OPSEC and contains the baseline implementation policies for roles, responsibilities, and requirements. The DoD Component policies that are listed below further define and apply more stringent OPSEC standards.

The OPSEC process generally involves analyzing friendly programs, projects, and activities to make sure that important information is not inadvertently shared with U.S. adversaries. To do this, OPSEC Managers identify CI and CILs. CILs can contain elements of information that are important to current operations, both tactical and strategic, that, if collected by U.S. adversaries, could endanger mission success. The smallest, most trivial details—even military materiel, building, and mission descriptions found in CRM reports—can be combined by U.S. adversaries to reveal larger plans and strategies and should be safeguarded. As such, OPSEC reviews of cultural resource information that is to be released to the public is required.

### ***Security and Policy Review of Information for Public Release***

The INFOSEC and OPSEC requirements in the DoD are the foundation of information management, whereas security and policy review is where the “rubber hits the road” and the procedures will affect the work of a CRM. At the DoD level, the Assistant Secretary of Defense for Public Affairs (ASD (PA)) and Under Secretary of Defense for Intelligence (USD(I)) share


the lead for the process of reviewing information for public release. As per this Instruction, and the related DoD Directives that drive it, it is DoD policy to perform security and policy reviews on all official DoD information intended for public release. This includes CRM reports that are shared with consulting parties, posted to the Internet, and even shared with other agencies.

**National Geospatial-Intelligence Agency**

NGA is responsible for GEOINT and for the National System for Geospatial-Intelligence (NSG)<sup>19</sup>, which ensures an overall compatible mapping system between agencies and follows the guidance of the Director of National Intelligence. The agency is also tasked with protecting intelligence sources and methods of information gathering from incurring an unauthorized disclosure.<sup>20</sup> The Director, NGA is appointed by the Secretary of Defense (if civilian) or the President (if military). All GIS and digital mapping work is subject to oversight of NGA and if such maps are planned for public release, they are required to undergo a security and policy review to ensure compliance with NGA requirements.

**DoD Component Documents**

The primary DoD policy statements concerning INFOSEC, OPSEC, and PA that are listed above are reflected in each of the DoD Component documents described below. The documents discussed below are the primary resources; however, there are additional sources that guide working with protected information in the annotated bibliography.



**U.S. Army**  
 Army Regulation 380-49  
 Army Regulation 380-5  
 HQDA, G2, Memorandum  
 Security Notice  
 Army Regulation 530-1  
 Army Regulation 360-1

*Annotated information for these resources is available in the bibliography.*

**U.S. Army**

**Army Regulation (AR) 380-5, Department of the Army Information Security Program (2000).**

This regulation implements the policy set forth in EO 12958, *Classified National Security Information*—with amendments—and DoD 5200.1-R, *Information Security Program*. It establishes the policy for classification, downgrading, declassification, and safeguarding of information requiring protection in the interest of national security. As such, it directly implements DoD and Federal Government requirements for Army INFOSEC. In addition to requirements concerning classification, handling, and declassification of information, this regulation provides procedures for CSMs, who are the primary point of contact (POC) for all classification issues. Army CSMs must ensure any document proposed for release outside Army control is reviewed

<sup>19</sup> This is a system that ensures standards and compatibility of mapping across agencies, it includes spatial data interface, metadata, and other aspects for an integrated system.

<sup>20</sup> Office of the Secretary of Defense, Director of Administration and Management. DoD Directive 5105.60, *National Geospatial intelligence Agency*, July 29, 2009, p. 5.

for potential classified information or CUI. You may find this regulation dense, but it is packed with information that is of direct import to the work of CRM—especially projects that relate to special weapons.

**AR 530-1, *Operations Security* (2007). FOR OFFICIAL USE ONLY – Limited Distribution**

This regulation provides details on the OPSEC planning process, and outlines OPSEC review, assessment, and survey. It specifies the need to determine an OPSEC Manager at a local / installation level, through whom all information slated for public release must be reviewed prior to publication.<sup>21</sup>

**AR 360-1, *The Army Public Affairs Program* (2011).**

This regulation includes requirements for PA offices to conduct security and policy reviews of Army documents that are intended for release to the public. It makes clear that PA is a command responsibility and that the role of PA is to fulfill the Army’s obligation to keep the American people and the Army informed. Under this regulation, any official information that is intended for public release—which pertains to military matters, NSI, or subjects of significant concern to the DoD—must be cleared by both an appropriate security review and PA office prior to release. Much of the information in this regulation does not directly apply to CRM work; however, if you are employed by or working with the Army you should become familiar with the regulation. It will help you to avoid issues and have more knowledgeable discussions with your PA.

***Department of Navy***

**SECNAV M 5510.36, *Department of the Navy Information Security Program Manual* (2006).**

This manual was developed to provide uniform implementation of INFOSEC program policy and procedures throughout the Department of the Navy (DON). It applies uniform, consistent, and cost-effective policies and procedures to the classification, safeguarding, transmission and destruction of classified information, as well as guidance on security education and the industrial security program. It applies to all DON commands and to all DON military and civilian personnel.

This manual defines roles and responsibilities. It is important to note that, “Military personnel are subject to disciplinary action under the Uniform Code of Military Justice, or criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of [the] policy manual.” And, “Civilian employees are subject to criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of [the] policy manual.”<sup>22</sup>

---

<sup>21</sup> This regulation is FOUO and was not available for the project team to use during the development of this handbook.

<sup>22</sup> Chief of Naval Operations (N09N), Special Assistant for Naval Investigative Matters and Security. SECNAV M 5510.36, *Department of the Navy, Information Security Program*, June 2006, p. 1-1.

It is important to become familiar with the contents of the manual so you can identify potential issues for your project(s) and work closely with your CSM to ensure proper review. As a department-level policy, this document also applies to the U.S. Marine Corps (USMC); further guidance for USMC activities can be found in the USMC Order P5510.18A, *USMC Information and Personnel Security Program Manual* (2000). If you are working with the USMC it will be important to become familiar with this document as well.



**U.S. Navy  
Information and Personnel  
Security**

SECNAV M-5510.36  
SECNAV 5510.36A  
SECNAV 5510.30B  
SECNAV M-5510.30  
DON Declassification  
Guide  
DON Declassification  
Manual

**OPSEC**  
OPNAVIST 3432.1A

**Public Affairs**  
SECNAVINST 5720.44C  
CHINFOINST 5720.8

*Annotated information for  
the resources on this sidebar  
is available in the  
bibliography.*

**U.S. Marine Corps  
Information Security**  
MCO P5510.18A W/Ch 1  
Marine Corps Warfighting  
Publication 3-40.2

**OPSEC**  
MCO 3070.2

**Public Affairs / Security  
and Policy Review**  
MCO 5230.18  
MCO 5720.77  
MCWP 3-33.3

**OPNAVINST 3432.1A, Operations Security (2011).**

This document establishes policy, procedures, and responsibilities for the Navy OPSEC program. It defines OPSEC for the Navy as a core competency that provides an integrated program for the protection of CI with the goal of disrupting, denying, and degrading the attempts of a U.S. adversary to gain an advantage. This document includes the enclosure “Navy OPSEC Program Management Responsibilities and Governance,” which outlines the roles for OPSEC Managers, the creation and protection of CI, and establishing that OPSEC Managers should review scopes of work prior to a public solicitation.

CRMs working with the USMC should consult their OPSEC Manager for current, specific policy and guidance for the USMC. The most recent USMC OPSEC policy at the time of publication of this handbook is MCO 3070.2, *The Marine Corps Operations Security (OPSEC) Program*, 18 May 2007.

**SECNAVINST 5720.44C, DON Public Affairs Policies and Regulations (2012).**

This document provides the basic policy and regulations for carrying out the PA and internal relations programs of the DON. It states that PA policy applies to all levels of DON and to all DON employees and that the principles of PA include “accountability to the public, full disclosure and expeditious release of information, alignment, and professional ethics.”<sup>23</sup> It includes detail on PA organization; information release policies; public information, internal communication, and community outreach; internet use; and communication products. You should become familiar with this

<sup>23</sup> Department of the Navy. SECNAVIST 5720.44C, *Department of the Navy Public Affairs Policy and Regulations*, 21 February 2012, p. 1-2.

document so you more fully understand the role of PA and integrating PA into your projects.

MCO 5720.77, *Marine Corps Public Affairs Order* (2007) is a parallel document for USMC that details PA processes and security and policy review. This document was developed to ensure that USMC also conducts both PA and security and policy reviews of their information. If you work with USMC, it will be important to become familiar with their documents, as well as DON.

### ***U.S. Air Force***

#### **Air Force Instruction 31-401, *INFOSEC Program Management* (2005).**

This Air Force Instruction (AFI) prescribes and explains how to manage and protect classified information and CUI. The AFI states that the protection of information is mission critical and that the goal is to review the information at the lowest levels possible. It also states that the Air Force will encourage and advocate the use of risk management principles; focus on identifying and protecting only that information that requires protection; integrate security procedures into Air Force business processes; and ensure all personnel understand their security roles and responsibilities.

Protection of information within the Air Force is accomplished primarily through the Air Force Information Security Program Manager—the security and policy reviews occur within the PA office of the Air Force (see AFI 35-102 below).

AFI 31-401 also states that if a historical researcher requires access to classified information, the researcher will be approved or disapproved by the Air Force Historian. The historian can be contacted at:

Air Force Historian (Headquarters USAF/HO)  
3 Brookley Avenue, Box 94  
Bolling AFB, DC 20032-5000

#### **AFI 10-701, *Operations Security* (2011).**

This AFI provides guidance for all Air Force personnel (military and civilian) and supporting contractors in implementing, maintaining and executing Air Force OPSEC programs. It describes the OPSEC process and discusses integration of OPSEC into Air Force plans, operations, and support activities. The instruction dictates the need for an OPSEC program at the local / installation level to ensure that all personnel such as website administrators, webmasters, supervisors, PA specialists, OPSEC coordinators, and others who review information for public release complete OPSEC training.



#### **U.S. Air Force *Industrial Security***

Air Force Policy  
Directive 31-6  
AFI 31-601

#### ***Information Security***

Air Force Policy  
Directive 31-4  
AFI 31-401

#### ***OPSEC***

Air Force Policy  
Directive 10-7  
AFI 10-701

#### ***Public Affairs / Security and Policy Review***

Air Force Policy  
Directive 35-1

**AFI 35-102, *Security and Policy Review Process* (2009).**

The Air Force INFOSEC program ensures that material proposed for public release is accurate, does not contain classified material, and does not conflict with established Air Force, DoD, or Federal Government policies. As noted above, the security and policy review process is completed within the PA program and clearance authority should always be delegated to the PA at the lowest echelon that is qualified to evaluate the contents and implications of your project. The PA organization with security and policy review authority will clear unclassified information of local or regional interest. The PA reviews speeches, presentations, papers, multimedia and visual information material, and information proposed for release to a publicly accessible Internet site.

**Summary**

As a CRM you should become familiar with the Federal, DoD, and DoD Component policies in order to follow the processes required to safeguard information from an unauthorized disclosure. This document synthesizes the processes for you, but you may also want to consult the source documents in order to better understand the impacts on your work.

The following sections describe the different types of information you or your contractor may be working with, the different reviewers you should be working with, and the typical issues that are associated with historical studies and CRM projects. This is intended to aid you in developing your project and to serve as a resource throughout the project process.



# CLASSIFICATION PRIMER

There are many types of data that require protection including data that were “previously restricted” and information that is unclassified, but controlled. It is important to familiarize yourself with the types of information that require protection and the basics of working with that information. Table 1 below is a list of the types of information that may affect your cultural resource project, each of these is described in this chapter.

**Table 1. Compilation of Information that Requires Protection**

Protected by E.O 13526*		Not protected by E.O. 13526	
National Security Information		Controlled Unclassified Information	
Non-Collateral	<b>Special Classified Information</b>		For Official Use Only
	Sensitive Compartmented Information		Sensitive But Unclassified
	Special Access Programs		Unclassified Controlled Nuclear Information
Collateral	<b>Classified Information</b>		Geospatial-Intelligence (unclassified)
	Restricted Data		Scientific and Technical Information
	Critical Nuclear Weapons Design Information		
	Formerly Restricted Data		
	Critical Technology		
	<b>Geospatial-Intelligence</b>		
	<b>Scientific and Technical Information</b>		
<b>Items that don't typically apply to CRM:</b>			
	<i>Non-Releasable to Foreign Nationals</i>		<i>Drug Enforcement Administration Sensitive Information</i>
	<i>Foreign Government Information</i>		<i>For Official Use Only Law Enforcement Sensitive</i>
			<i>Caution-Proprietary Information Involved</i>
<i>*Except for those items that are protected under the Atomic Energy Act and its implementing laws (as noted above).</i>			

## National Security Information

NSI consists of any official information that has been determined under an EO to require protection against unauthorized disclosure and has been designated as such. This also includes non-military information that should be classified in the “interest of national security.” Should your project involve the use of NSI, it will require a special contract type; consultants or personnel with the appropriate clearance level; and, most likely, result in a longer schedule and larger budget. The project schedule and budget implications will arise from the information access protocols and require upper echelon and / or outside agency security and policy reviews. As a result, it is highly likely that there will be more participants in your project, there will be more reviews, and it will require more management than the typical cultural resource project. In addition, the contractor will be required to handle NSI information that is in their custody using specific guidance provided by your DoD Component.<sup>24</sup> You should be aware of the potential implications to your project when you are planning the funding and developing a contract—this

<sup>24</sup> DoD Manual, 5200.01, *DoD Information Security Program: Overview, Classification, and Declassification*, Volume I, Enclosure 5, p. 55.

section provides a basic understanding of the types of classified information, and the subsequent sections provide information on DoD reviews, contracts, and other items that will affect your work.

### **Security Classification Guidance**

For each of the types of classified information, there are SCGs. OCAs are responsible to develop SCGs to aid providing effective and efficient INFOSEC measures. They are required to develop an SCG for each system, plan, program, or project that involves classified information; they are also responsible to review and update the SCG as necessary. SCGs can be developed for classified information or CUI and should themselves be treated as CUI—they are subject to the Freedom of Information Act (FOIA), but the only releasable sections are those that do not detail specific items that are classified or the reasons for their classification. SCGs are to be written as early as possible during the development of military materiel or systems, so if a CRM or contractor is writing a historical study, if it touches on classified information, it is highly likely that an SCG has previously been developed. SCGs include:

1. Specific items or elements of information that must be protected.
2. Classification assigned to each item or element.
3. Concise reason for classifying an item or element.
4. Declassification instructions for each item or element, including exemptions from automatic declassification.
5. Special handling caveats, such as dissemination controls or restricting posting of elements to the Internet.
6. Identification of the OCA, including name, title, and date of approval.
7. A POC for questions about the SCG.<sup>25</sup>

SCGs are to be distributed to organizations that may classify information that is covered by the guide, as well as DOPSR and Defense Technical Information Center (DTIC). An index to the guides is located on DTIC and the guides are reviewed every 5 years to ensure the information is current. SCGs are revised as necessary and any changes to the guides are reported to DTIC using Defense Department (DD) Form 2024. If the SCG is deemed out-of-date, it is removed from the index and DTIC. SCGs are cancelled when the information in the guide has become declassified or a new guide covers the information that is included in an old guide. Copies of defunct SCGs are not kept by DTIC or DOPSR; however, the OCA is meant to maintain copies of cancelled guides.<sup>26</sup> Although OCAs are meant to keep copies of outdated SCGs, using one

---

<sup>25</sup> DoD Manual, 5200.01, *DoD Information Security Program: Overview, Classification, and Declassification*, Volume I, Enclosure 6, pp. 71-72.

<sup>26</sup> *Ibid.*, p. 73.

inadvertently could result in illegally protecting information—that is, classifying something that should not be—so it is likely that old SCGs have been destroyed to ensure they are not used.

## Special Classified Information

### *Sensitive Compartmented Information*

Sensitive Compartmented Information (SCI) is classified information that concerns or is derived from intelligence sources or methods, or analytical processes—SCI consists of our nation’s most valued and closely guarded assets.<sup>27</sup> SCI is required to be handled within formal access control systems—investigations and determinations of who is eligible to view the information—that are established by the Director of National Intelligence. Having a clearance that allows for access to SCI can be characterized as a level that is “above Top Secret.” The same investigation is required for SCI as for Top Secret; however, obtaining clearance for SCI does not mean eligibility to view all SCI—explicit permission for specific information must also be obtained.

*TIP: Become familiar with the types of safeguarded information and classification policies so you know whether you will need to access such information to meet your duties, can recognize the markings, and better understand how to treat the documents in your possession.*

As an example, in the mid-1950s the entire U-2 program was considered SCI—such a program could be a topic of a Cold War study, so it is possible that past SCI may apply to a cultural resource project. It seems unlikely that current SCI would be involved in a cultural resource project; however, if SCI applies, there are numerous considerations that will affect your project viability—such considerations are discussed in the following sections and it will be important to understand these implications prior to initiating work.

### *Special Access Programs*

DoD SAPs are activities with enhanced security measures that impose safeguarding and access requirements exceeding those that are normally required for information at the same level. They are established and maintained only when absolutely necessary to protect the most sensitive DoD capabilities, information, technologies, and operations. A SAP may also be required by statute. Information that is to be protected within the SAP is identified by an SCG.<sup>28</sup>

There are two types of DoD SAPs: acknowledged and unacknowledged. The existence of acknowledged SAPs can be made public in unclassified settings, even though the details of the program will remain highly classified. An unacknowledged SAP has enhanced security measures to ensure the existence of the program is not acknowledged, affirmed, or made known to any person that is not authorized for such information. In addition to the heightened levels of security measures to protect information about SAPs, other programmatic aspects—such as

<sup>27</sup> United States Government Accountability Office. *Defense Critical Infrastructure: DOD’s Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets*, GAO-08-373R Defense Critical Infrastructure, April 2, 2008, p. 2.

<sup>28</sup> Department of Defense, Special Access Program Central Office. DoD Instruction 5205.11, *Management, Administration, and Oversight of DoD Special Access Programs (SAPs)*, February 6, 2013.

specialized non-disclosure agreements, special terminology or markings, and exclusion from standard contract investigations—may apply.

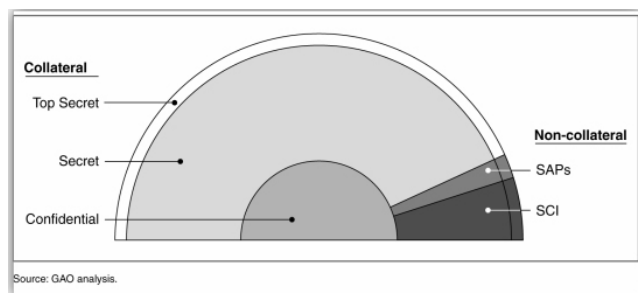
As a CRM, it is highly unlikely that you or your contractor will encounter current SAPs—especially unacknowledged SAPs—either during the planning or implementation phases of a project. You should be aware that they exist and be prepared to ask your ASM/CSM, OPSEC Manager, and / or PAO if the work you plan to accomplish is connected in any way to a current or historical SAP. If so, you should seek the ASM/CSM’s guidance on how to proceed with the project, most likely by changing the project scope and requirements to avoid SAPs entirely, if possible.

### Classified Information

Classified information is that which is identified as requiring protection against unauthorized disclosure in the interest of national security. There are three levels of classified information:

1. Top Secret: this level is applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.
2. Secret: this level is applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe.
3. Confidential: this level is applied to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the OCA is able to identify or describe.”<sup>29</sup>

Each of the above classification levels can apply to the information types that are described below. There are also two distinctions of classified information: collateral and non-collateral.



Collateral information is that which is identified as NSI under the provisions of EO 13526, but which is not subject to enhanced security protection required for SCI. SCI is “compartmented information,” separated from collateral information and is considered non-collateral.

**Figure 2. The Relationship between Collateral and Non-Collateral Designations**

Note: The areas that are shown here represent categories of NSI. All classified information is Confidential, Secret, or Top Secret. Information classified at these levels but not subject to any additional safeguarding and access

<sup>29</sup> DoD Manual, 5200.01, *DoD Information Security Program: Overview, Classification, and Declassification*, Volume I, Enclosure 4, p. 34.

requirements is collateral information. Some information that is classified Secret or Top Secret also falls under an SCI or SAP designation; that information then becomes non-collateral. The relative size of each area is illustrative only.<sup>30</sup>

### ***Restricted Data***

Restricted Data (RD) is all data that concerns the: 1) design, manufacture, or utilization of atomic weapons; 2) production of special nuclear material (SNM); or 3) use of SNM in the production of energy. Information can be removed from the RD category under the provisions of Section 142 of the Atomic Energy Act of 1954, as amended; this however, does not necessarily mean the information has become declassified, but it does mean that it has been recategorized. Section 142 of the Atomic Energy Act includes provisions for the Department of Energy (originally the Atomic Energy Commission) to:

1. Maintain a continuous review of RD and associated SCGs to allow for its removal from the RD category.
2. Collaborate with the DoD with regard to information removal from the RD category. If the two agencies do not agree on removal or re-categorization, the determination is made by the President.
3. Remove information from the RD category; however, information that has been removed will not be shared with foreign entities so long as it remains “defense information”—unless there has been a previous agreement between the foreign entity and the U.S.
4. Collaborate with the Director of National Intelligence to jointly determine the RD categorization of information concerning the atomic energy programs of other nations—under the provisions of Section 102(d) of the National Security Act of 1947, as amended—this section defines the roles of the Director of National Intelligence.<sup>31</sup>

It is unlikely that RD will be a critical component of a cultural resource report; however, such work may touch upon the “utilization” of atomic weapons in a way that may require access to classified information.

### ***Critical Nuclear Weapons Design Information***

Critical Nuclear Weapons Design Information (CNWDI) includes RD information that has been categorized at the levels of Top Secret or Secret. CNWDI reveals the theory of operation or design of the components of a thermonuclear or implosion type fission bomb, warhead, demolition munitions, or test device. The sensitivity of CNWDI is such that it is in the national interest to assure that access is granted to the absolute minimum number of employees who require it in order to accomplish their assigned responsibilities on the strictest need-to-know basis. As such, access is granted only to those who have a Final Top Secret or Secret clearance.

<sup>30</sup>U.S. Government Accountability Office. GAO-08-373R, *Defense Critical Infrastructure: DOD’s Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets*, p. 2.

<sup>31</sup>U.S. Regulatory Commission. Nuclear Regulatory Legislation, 112th Congress; 2nd Session, NUREG-0980, Vol. 1, No. 10., pp. 83-84.

It is highly unlikely that CNWDI will be a critical component of a cultural resource report. Should it be necessary, there would be numerous considerations that will affect your project viability, contract type, budget, and schedule. It will be important to understand these implications when designing your project.

### ***Formerly Restricted Data***

Formerly Restricted Data (FRD) is information—relating primarily to the military utilization of atomic weapons—that was removed from the Department of Energy (DOE) RD category upon a joint determination by the DOE (or its antecedent agencies) and the DoD. Such removal from the DOE RD category does not mean that the data is declassified, but rather that the FRD information status has changed and can be adequately safeguarded as classified defense information. For purposes of foreign dissemination, FRD information is treated in the same manner as RD.

It is likely that if you have a classified project, you or your contractor could be working with FRD. This would require the appropriate clearance and will affect the parameters of your project.

### ***Critical Technology***

The idea of identifying certain U.S. commodities as “critical” began in the 1920s when the Government realized that a dependence on the foreign import of certain materials created vulnerability for the U.S. military. As a result, Congress required that the U.S. maintain a strategic reserve of such “critical materials” in order to ensure readiness in case of military conflict. An extension of the concept was that some technologies are critical for military readiness and some technologies support economic growth—this resulted in the use of the term “critical technologies” in the 1990 Public Law 101–189, which mandated a critical technologies report. In this law, Congress defined critical technologies as “essential for the United States to develop to further the long-term national security or economic prosperity of the United States.”<sup>32</sup>

Since 1990, the U.S. has been protecting critical technologies and the DoD has developed and maintained a Military Critical Technology List (MCTL). The purpose of the MCTL is to identify and assess technologies that are critical for retaining U.S. military dominance.<sup>33</sup> Such technologies are defined as: 1) arrays of design and manufacturing know-how (including technical data); 2) keystone manufacturing, inspection, and test equipment; 3) keystone materials; and 4) goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or

---

<sup>32</sup> U.S. Government Printing Office. 42 United States Code, 1999 Edition, *Title 42—The Public Health and Welfare Chapter 79—Science and Technology Policy, Organization, and Priorities, Subchapter VI—National Critical Technologies Panel*, §6683—Biennial National Critical Technologies Report, subsection (b).

<sup>33</sup> U.S. Government Accountability Office. *Report to Congressional Committees, Protecting Defense Technologies: DOD Assessment Needed to Determine Requirement for Critical Technologies List*, GAO-13-157, January 2013 p. 23.

combination of countries and that may prove detrimental to the security of the U.S. (also referred to as militarily critical technology).

Of all the NSI, critical technology is the most likely to be included in your cultural resource project. The mere mention of a technology is probably not protected; however, should you go into detail about the specifications and technical details you would be revealing protected critical technology. Studies that include military materiel, test ranges, etc. may include information that is on the MCTL and may require information protection. If you believe that technology on the MCTL will be included in your project, be sure to contact your PA, OPSEC Manager, and ASM/CSM to ensure they are aware of your project and to obtain their input into its development. If the work is to be contracted, be sure your Contracting Officer is notified that you believe MCTL information will be included.

### Geospatial-Intelligence

GEOINT is the analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically-referenced activities on the Earth. GEOINT includes imagery, imagery intelligence, and geospatial information and can include data and information from collateral sources. The Secretaries of the Air Force, Army, Navy, and USMC are responsible for designating GEOINT elements to facilitate integrating GEOINT-related activities and military service functions across the NSG. The designated element serves as the formal service POC for all military service GEOINT functions and activities, including NSG planning, programming, budgeting, acquisition, technology investment, policy, doctrine, training, tradecraft, personnel, tasking, collection, process, production, exploitation, and dissemination.<sup>34</sup>

With regard to GEOINT, the Heads of the DoD Components:

1. Assign responsibilities and establish procedures, as appropriate, within their Component to implement DoD Instruction 3115.15, *Geospatial Intelligence*.
2. Coordinate with the USD(I) and the Director, NGA when the Component proposes or oversees new GEOINT-related activities or programs.
3. Identify classified information and provide SCGs for all DoD airborne and DoD spaceborne GEOINT data, sensors, and systems that are developed within their organizations, as well as determine the foreign disclosure and release parameters for the above materiel.<sup>35</sup>
4. Manage and submit requirements, programming, and execution for GEOINT in accordance with the Joint Chiefs of Staff (JCS) Instruction, 3901.01C, which provides guidance for a

---

<sup>34</sup> Ibid., p. 10.

<sup>35</sup> Under Secretary of Defense for Intelligence. DoD Instruction 3115.15, *Geospatial Intelligence*, Enclosure 2, p. 12. Disclosure is determined through DoD Directive C-5230.23, *Intelligence Disclosure Policy (U)*, November 18, 1983 and DoD Instruction 5000.56, *Programming Geospatial intelligence, Geospatial Information and Services, and Geodesy Requirements for Developing Systems*, July 9, 2010.

strategy to consolidate and prioritize geospatial information and services requirements to ensure optimal use of production resources. JCS Instruction 3901.01C also guides priorities for the Combatant Commands, Military Services, Chairman of the JCS, and other NSG members in support of military operations.<sup>36</sup>

## **Scientific and Technical Information**

Scientific and Technical Information (STINFO) is a type of unclassified information that you may encounter while managing a cultural resources program. STINFO is generally affiliated with research, development, test, and evaluation (RDT&E), research and engineering (R&E), and science and technology (S&T) transfer programs. At the DoD level, the STINFO Program (STIP) is managed by the Director, Defense Research and Engineering—as the Principal Staff Assistant to the Under Secretary of Defense for Acquisition, Technology and Logistics. Each DoD Component also has a STINFO program. Policy, guidance, and references for these programs can be found in the bibliography.

Dissemination of accurate, complete, and timely STINFO is the major impetus that drives the DoD STIP. DoD Components appoint managers to oversee STINFO programs at the local level. This manager ensures that every appropriate defense effort is reported under the Research Awareness Initiative, and that technical publications generated from efforts are properly disseminated. The goal is to eliminate unnecessary duplication of effort and resources by encouraging and expediting the interchange and use of STINFO, which is intended to include DoD Components, their contractors, other Federal agencies, their contractors, and the national and international scientific community.<sup>37</sup>

As a CRM, you or your contractors will not be generating STINFO, as your work does not fall into the definition of an RDT&E, R&E, or S&T program. However, you may find that aspects of your research into a given facility, program, activity, etc. may include information that does qualify as STINFO. DoD and the DoD Components have strict guidance for how STINFO reports are created, reviewed, and disseminated, so it is important to work with a properly cleared DoD document, which would include a Distribution Statement on the cover and title page and a completed Standard Form (SF) 298 in the report.<sup>38</sup>

If you include STINFO in your document, be sure it comes from cleared / authorized sources; although it is possible you may be working with an uncleared STINFO report. You should consult the DTIC STINFO site; as part of its STIP training initiative, DTIC provides several resources useful to the research and production of CRM documents, including a current list of all

---

<sup>36</sup> DoD Instruction 3115.15, *Geospatial Intelligence*, p. 9; JCS Instruction 3901.01C, *Requirements for Geospatial Information and Services*, April 10, 2010, Enclosure A, p. A-1.

<sup>37</sup> Director of Defense Research and Engineering. DoD Directive 3200.12, *DoD Scientific and Technical Information Program*, 11 February 1998, pp. 2-3.

<sup>38</sup> See the Project Process, Phase IV section of this report for more information on Distribution Statements and SF 298s.



relevant policy, guidance, and reports.<sup>39</sup> If you are in doubt as to the status of a document you produce, you should ask your ASM/CSM to connect you with the STINFO Program Manager to seek more advice. The standard document reviews discussed elsewhere in this report (by ASM/CSM, OPSEC Manager, and PA) will also take STINFO into account.

### **Controlled Unclassified Information**

CUI is unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulation, and Government-wide policies. CUI is defined and governed by laws, international agreements, EOs, and regulations that address the identification, marking, protection, handling, transmission, transportation, and destruction of such information. Categories of CUI—in the order of likely applicability for cultural resource projects—include:

1. For Official Use Only (FOUO): unclassified information that requires protection, as defined under FOIA.
2. DoD and DOE Unclassified Controlled Nuclear Information (UCNI)<sup>40</sup>: unclassified information that could reasonably be expected to have a significant adverse effect on: a) the health and safety of the public or b) the common defense and security by significantly increasing the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD materiel.
3. DOS Sensitive But Unclassified (SBU) (formerly Limited Official Use, also known as LOU) information.
4. Law Enforcement Sensitive Information (LES).
5. Drug Enforcement Administration Sensitive Information.
6. NGA: imagery produced by NGA that requires a limited distribution.
7. Unclassified information in technical documents that require distribution statements.

Although the implementation of the National CUI program has not occurred, the DoD Manual 5200.01, Volume 4 is EO 13556 aware. All DoD personnel should follow the guidance contained in Volume 4 for all things CUI to include the terms FOUO, DoD UCNI, SBU, LES, etc...once DoD implements EO 13556 those terms will become legacy terms and new directives, regulations, and instructions will apply.

The markings for the different categories of CUI in documents are noted in Table 2. This information is provided so that in the event you or your contractor find such markings, you will

---

<sup>39</sup> <http://www.dtic.mil/dtic/customer/training/stinfo/stinfodocs.html>

<sup>40</sup> DOE UNCI is referred to as just UNCI, while DoD UNCI is always referred to as DoD UNCI. Once CUI is in place, UNCI and DoD UNCI will remain applicable terms and types of protected information.

be clear on their use and meaning. If you are working with a video, display, or other media—refer to DoD Manual 5200.01, Volume 4, Enclosure 3 which identifies similar markings.

**Table 2. CUI Markings**

MARKINGS	OUTSIDE			INSIDE				
	Bottom Outside Front Cover	Title and First Page	Outside Back Cover	Subject	Titles	Section, Part, or Paragraph	Bottom of Page with Info	Originating Office Noted
<b>UNCLASSIFIED DOCUMENTS</b>								
“FOR OFFICIAL USE ONLY”	√	√	√				√	
FOUO				√	√	√		√
“DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION”	√	√	√				√	
“DOD UNCI” (DNCI)	√	√	√				√	
“SENSITIVE BUT UNCLASSIFIED” (SBU)	√	√	√	√	√	√		√
“SENSITIVE BUT UNCLASSIFIED NOFORN” (SBU NOFORN)	√	√	√				√	
“SBU NOFORN” (SBU-NF)	√	√	√				√	
<b>CLASSIFIED DOCUMENTS</b>								
<i>Pages with no classified information, but have CUI</i>								
FOUO				√	√	√		√
“UNCLASSIFIED//DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION”	√	√	√				√	
“UNCLASSIFIED//DOD UCNI” (U//DCNI)	√	√	√				√	
<i>Pages with classified information and DCNI</i>								
(S//DCNI)				√	√	√		

### For Official Use Only

FOUO is a dissemination control to protect information that if provided to the public would be expected to cause foreseeable harm to U.S. interests; it is not meant to protect information that otherwise would not merit national security protection. FOUO is applied by the DoD to unclassified or declassified information and may also appear within a classified document. Marking information as FOUO will not automatically qualify it for exemption from public release under FOIA. If a request for a record is received, the information will be reviewed to determine if it truly qualifies for exemption. Conversely, the absence of the FOUO marking does not automatically mean the information shall be released—for example, records such as personnel documents, are not normally marked FOUO, but may still qualify for withholding in accordance with the FOIA.

The primary consideration during research and project development is that if research materials are marked FOUO, the information cannot be released to the public. If you include it in a CRM

report that is planned for release, you are creating a problem before the document even gets to a draft stage.

The originator of a document is responsible to determine whether the information may qualify for FOUO status and to ensure that markings (as noted in Table 2) are applied as required. In order to be considered FOUO, the information must meet one or more of the exemptions of FOIA.<sup>41</sup>

### ***Freedom of Information Act***

The marking “FOR OFFICIAL USE ONLY” is applied to information that can reasonably be expected to qualify for exemption under one or more of FOIA Exemptions 2 through 9.<sup>42</sup> The eight FOIA exemptions that apply to FOUO are as follows:

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 memorandums or letters containing information considered privileged in civil litigation. The most common privilege is the deliberative process privilege, which concerns documents that are part of the decision-making process and contain subjective evaluations, opinions, and recommendations. Other common privileges are the attorney-client and attorney work product privileges.

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 that:

- a. Could reasonably be expected to interfere with law enforcement proceedings.
- b. Would deprive a person of a right to a fair trial or impartial adjudication.
- c. Could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others.
- d. Disclose the identity of a confidential source.

<sup>41</sup> The U.S. Department of Justice. FOIA Update, Vol. XVII, No. 4, 1996, *The Freedom of Information Act*, 5 U.S.C. §552, As Amended By Public Law No. 104-231, 110 Stat. 3048, subsection (b), items (2) through (9).

<sup>42</sup> Exemption 1 applies to information that is currently and properly classified. However, a classified document may contain pages or paragraphs with FOUO information and these portions of a classified document may remain FOUO after declassification.

- e. Disclose investigative techniques and procedures.
- f. Could reasonably be expected to endanger the life or physical safety of any individual.

Exemption 8. Certain records of agencies responsible for supervision of financial institutions.

Exemption 9. Geological and geophysical information (including maps) concerning wells.<sup>43</sup>

For a more detailed list that applies to directly your DoD Component, contact your FOIA office. They will have information about exempt resources that are protected under the National Historic Preservation Act of 1966 and Archaeological Resources Protection Act of 1979.

### ***Access***

In order to obtain access to FOUO, a person must have been determined to have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose. The final responsibility for determining whether someone may have access to the data lies with the individual who has the “authorized possession” of the information. FOUO information can be disseminated within the DoD Components and their contractors, consultants, and grantees when necessary to conduct official business for the DoD; however, this must be consistent with the controls imposed by a document *distribution statement*.<sup>44</sup> It is also possible to share FOUO with foreign governments and international organizations, as long as the distribution is in compliance with applicable statutes, regulations, and policies.

Records that are released outside of the DoD should be reviewed to determine whether the information warrants FOUO status. FOUO information can be shared with State, local, or tribal government officials. In order to share the information such sharing must be in “furtherance of an official government purpose” and a specific need-to-know must be established. In all cases, the recipient must agree to the stipulation that the information shall be withheld from release to the public by the State, local, or tribal recipient. Records must be appropriately marked and the recipient must be advised on special handling instructions.<sup>45</sup>

### ***Protection***

FOUO must be protected during and after work hours. During work you must take reasonable steps to minimize unauthorized personnel access—for example, it is important to never leave FOUO unattended or to read or discuss FOUO where unauthorized personnel may be present. After work, if your building has Government or Government-contract building security, you can store FOUO in unlocked containers, desks, or cabinets. If your building does not have such security, the information must be stored in a locked location.

<sup>43</sup> DoD Manual, 5200.01, *DoD Information Security Program: Controlled Unclassified Information*, Volume 4, Enclosure 3, pp. 11-13.

<sup>44</sup> See Phase IV of the Project Process section of this report for more information on distribution statements.

<sup>45</sup> DoD Manual, 5200.01, *DoD Information Security Program: Controlled Unclassified Information*, Volume 4, Enclosure 2, p. 16.

You can transmit FOUO information by first class mail or parcel post. You can transmit FOUO by a website or email if it is an approved secure communications system or system utilizing other protective measures such as Public Key Infrastructure or transport layer security, such as https://. Additional protocols apply if you are going to upload FOUO to websites (see DoD Manual 5200.01, v. 4). Use of wireless telephones should be avoided, but you can use a facsimile machine (fax) as long as the receiver is at the receiving location when transmission begins. In addition, record copies of FOUO documents must be disposed of under the provisions of United States Code (U.S.C.), Title 44, Chapter 33 and the records management directives of your DoD Component. Non-record FOUO documents may be destroyed by any of the means approved for the destruction of classified information or by any other means that would make it difficult to recognize or reconstruct the information.<sup>46</sup>

### **Unclassified Controlled Nuclear Information**

This category of CUI is exempt from FOIA and is protected to prevent the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, SNM equipment, SNM facilities, or nuclear weapons in DoD custody. DoD UCNI consists of unclassified information on security measures for the physical protection of DoD SNM when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security of the U.S. Such information is designated as DoD UCNI by heads of the DoD Components or authorized delegated individuals.<sup>47</sup>

#### ***Access***

Access to DoD UCNI is granted only to those who have a valid need-to-know and are specifically eligible for access in accordance with DoD Manual 5200.01. Those who are granted access must be made aware of the DoD UCNI status of the information and the transmission of the information must be by means that preclude unauthorized disclosure or dissemination. Those who are DoD authorized holders of DoD UCNI are authorized to convey such information to officials in other U.S. departments or agencies on a need-to-know basis if the purpose is to fulfill a Government function.

#### ***Protection***

When not commingled with classified information, DoD UCNI may be sent by first-class mail in a single, opaque envelope or wrapping. Transmission of DoD UCNI must only be completed using approved, secure communications circuits and equipment (telephone, email, facsimile), except in the event of an emergency.

---

<sup>46</sup> Ibid., p. 18.

<sup>47</sup> Ibid., p. 20.

As with FOUO, DoD UCNI must be protected during and after work hours. During work you need to take reasonable steps to minimize unauthorized personnel access—for example, it is important to never leave DoD UCNI unattended or to read or discuss DoD UCNI where unauthorized personnel may be present. After work, if your building has Government or Government-contract building security you can store DoD UCNI in unlocked containers, desks, or cabinets. If your building does not have such security, the information must be stored in a locked location.

Copies you may have of DoD UCNI (unless you are at the DoD Component level) are considered “non-record” and once you are done using them you can destroy them by shredding, burning, or by any of the other means approved for the destruction of classified information.<sup>48</sup>

### **Sensitive But Unclassified**

SBU information was previously known as “Limited Official Use” information and it is exempt from FOIA. SBU is information that originated within the DOS and warrants a degree of protection and administrative control. If a document contains both DOS SBU and FOUO information, the SBU markings supersede FOUO in the markings at the bottom of the cover and title pages and at the bottom of internal document pages.

#### ***Access***

Within the DoD, the criteria for allowing access to DOS SBU information are the same as those used for FOUO information, except that information marked “SBU NOFORN” (or portion marked “(SBU-NF)”) shall not be provided to any person who is not a U.S. citizen without the approval of the DOS activity that originated the information.

#### ***Protection***

Within the DoD, DOS SBU information shall be protected in the same manner as that required for DoD FOUO information.<sup>49</sup>

### **Geospatial-Intelligence (Unclassified)**

Unclassified GEOINT that is derived from NGA materials in the possession of, or under the control of DoD may be withheld from public release if it:

1. Was obtained, produced, or contains information that was provided in accordance with an international agreement that restricted the disclosure of the information to only the agreeing parties’ Government officials or if the agreement restricts such information for DoD or Government use only.

---

<sup>48</sup> Ibid., pp. 21-22.

<sup>49</sup> Ibid., pp. 24-25.

2. Contains information that the Secretary of Defense has stated in writing that if it were disclosed it would reveal the sources, methods, or capabilities used to obtain source material for the production of GEOINT.
3. Contains written information that the Director, NGA has stated in writing that if it were disclosed it would jeopardize or interfere with ongoing military or intelligence operations; reveal military operational or contingency plans; or reveal, jeopardize, or compromise military or intelligence capabilities.<sup>50</sup>

It is also the responsibility of the Director of NGA to determine if any other GEOINT under the control and in the possession of DoD warrants similar protection. If GEOINT is withheld from public release for any of the above reasons or the Director of NGA determination, the material will be marked, “LIMITED DISTRIBUTION” and will include any additional markings that have been established by the NGA. If NGA-produced material has been marked LIMITED DISTRIBUTION GEOINT, it will be provided FOUO to the DoD Components and to authorized DoD contractors who may require the material for use in the performance of DoD contracts. The material will be provided in accordance with U.S.C. Title 48 of the Federal Acquisition Regulations (FAR) System, § 245 and § 252, which govern the chain of custody and how such material should be handled.<sup>51</sup>

If information marked LIMITED DISTRIBUTION GEOINT or any products derived from such information is planned for public release or dissemination to other agencies outside the DoD, it must be approved in writing by the Director of NGA or his delegated authority, the Director of the Office of International Policy. If you have a situation where you are anticipating public release of such limited distribution information, you will need to make a request in writing and mail it to:

NGA, Office of International Policy  
NGA Main Office Building  
7152 Heller Loop  
Springfield, VA, 22150-3164

### **Changes in Classification**

The status of national security information that has been classified can also be changed—information that has been classified does not remain so indefinitely. When it is classified, the OCA sets a date when the document should automatically be declassified, but there can be other factors which trigger changes up or down in the classification level. In addition, when conducting archival research, you may find a document that should have been automatically

---

<sup>50</sup> Under Secretary of Defense for Intelligence. DoD Instruction, 5030.59, *National Geospatial intelligence Agency LIMITED DISTRIBUTION, Geospatial Intelligence*, pp. 2-3.

<sup>51</sup> Ibid. and DoD Manual, 5200.01, *DoD Information Security Program: Controlled Unclassified Information*, Volume 4, Enclosure 3, pp. 22-24.

declassified, but was not. Requests can be made to review the status of a document and alter its classification.

## Declassification

Information is intended to be declassified once it no longer meets the standards for classification, but it can also be declassified if the public interest outweighs the need for keeping the information classified. The latter occurs in exceptional cases and requires a senior agency official to make the determination. In either case, there are specific personnel who may declassify information:

1. The OCA, or the supervisory officials of the OCA, with jurisdiction over the information (classification, program, or functional responsibility).
  - a. If an activity that originated the classified information no longer exists, the declassification authority transfers to the organization that inherited the functions of that activity.
  - b. If the activity functions were dispersed or ceased, the authority transfers to the DoD Component under which the activity functioned.
2. DoD Component Heads with OCA—they can also designate officials within their organization to act in this capacity.
3. Information that originated with another agency should be referred to that agency's originator for declassification decisions.<sup>52</sup>

Personnel who have declassification authority also have the responsibility to develop and issue guidance to allow for the effective review and declassification of NSI. Such guidance may appear in memorandums, SCGs, or in a separate declassification guide. Documents that have been declassified are required to have markings that identify declassification status and who authorized the declassification. In general, there are four processes for declassifying information:

1. The OCA determines a date when the information should be declassified. Once the document reaches that date, the authorized holder of the information must confirm with the OCA that the date has not been extended. Until this has been completed, the information must continue to be classified.
2. Records of permanent historical value automatically is declassified 25 years from the date of origin (unless specific steps are taken to keep the information classified).

---

<sup>52</sup> DoD Manual, 5200.01, *DoD Information Security Program: Overview, Classification, and Declassification*, Volume I, Enclosure 5, p. 52-53.



3. Mandatory Declassification Review. If an authorized holder of the information believes that it is not properly classified, the OCA is notified through proper channels. The information remains protected until the issue is resolved.
4. Systematic review for possible declassification. Within a DoD Component there are systematic reviews of records of permanent historical value that are subject to and have been exempted from automatic declassification; the reviews are prioritized by the National Declassification Center. At NARA, all records of permanent historical value are slated for declassification review by December 31 of the year in which they become 25 years old. Unless the document warrants continued protection, it is declassified. Although they are slated for review, many times the deadline may have been pushed back. In which case, if you need the document you may ask for a mandatory declassification review.

Any individual or organization can request a declassification review—DoD Components have processes to handle such requests and there may be fees associated with such a request. The DoD Component can review the information as long as they are provided with a specific request and enough information to find the records with a “reasonable amount of effort.” If you or your contractor make a request for an entire series of documents or do not have sufficient locational information, your declassification request may be denied. Also, NSI that may affect another agency will be referred to that agency for review prior to declassification, which could cause a time delay in the declassification request. If the information is subject to pending litigation or has been reviewed within the past 2 years, the request will be denied (although it is possible to appeal the review of information that was reviewed within the past 2 years). If you do make a request, the DoD Component will provide a prompt decision or advise you that additional time is needed to make the determination. If the entire document cannot be released, the DoD Component will make a reasonable effort to release the portions of the document that are no longer classified and redact those that are.<sup>53</sup>

*TIP: Understanding declassification processes can aid you and your contractor in accessing information that should be declassified, but was somehow overlooked through the years. Requests for a revision of classification may add time to your project, but could result in a more detailed project with better historical insight.*

Classified information must be marked as “declassified” before it can be handled as unclassified information. In order to declassify—even if there is a declassify date noted on the document—the authorized holders of the information must confirm with the OCA that the date has not been extended. There can be reasons that information should be protected for a longer period than originally anticipated and there are numerous exemptions that can be applied to prevent automatic declassification.<sup>54</sup> Once the information has been declassified, it is not automatically

<sup>53</sup> Ibid., pp. 64-66.

<sup>54</sup> For more information on exemptions see Enclosure 5, pp. 59-64 of DoD Manual, 5200.01, *DoD Information Security Program: Overview, Classification, and Declassification*, Volume I.

released to the public. It must go through a review to ensure that there are no reasons to withhold the information—it is possible that declassified information may contain CUI.

There also may be delays to automatic declassification for items that are presented in a media format that is difficult or costly to review, such as records that require extraordinary preservation or conservation treatment (declassification process may cause damage), records that may have the potential to harm health due to contamination from a harmful substance, electronic media that is subject to obsolescence, or degraded data.

## **Duration of Classification**

### ***Declassification Date***

When a classified document is created, the OCA determines how long the information must be protected and this is published in the appropriate classification / declassification guide or in a specific SCG.<sup>55</sup> The OCA also will define a declassification date or event—a point in time when it is anticipated that the information will lose its sensitivity or when an event occurs that alters the sensitivity of the information. The OCA will assign a duration option and is expected to use the option that will both protect the information and result in the shortest duration of classification. The following are the current options:

1. A date or independently verifiable event less than 10 years from the date of the document;
2. A date 10 years from the date of the document;
3. A date or independently verifiable event greater than 10 and less than 25 years from the date of the document;
4. A date 25 years from the date of the document;
5. “50X1-HUM,” designating a duration of up to 75 years, when classifying information that could clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source;
6. “50X2-WMD,” designating a duration of up to 75 years, when classifying information that could clearly and demonstrably be expected to reveal key design concepts of non-nuclear WMD; or
7. “25X” with date or event, designating a duration of up to 50 years when classifying information that clearly falls within an exemption from automatic declassification at 25 years that has previously been approved by the Interagency Security Classification Appeals Panel.<sup>56</sup>

---

<sup>55</sup> DoD Manual, 5200.01, *DoD Information Security Program: Overview, Classification, and Declassification*, Volume 1, Enclosure 4, p. 38.

<sup>56</sup> *Ibid.*, p. 40-41.

### ***Extending the Duration of Classification***

Information will be declassified on the date or event specified by the OCA. However, the date of declassification can be extended if the date of declassification has not passed and the information continues to meet standards for classification. However, the period of classification cannot exceed 25 years from the original document date. Once the date is extended, all authorized holders of the document must be notified of the extension.

If the date or event specified by the OCA has passed, the information may be reclassified only if there is a compelling national security reason and if the information can reasonably be recovered.<sup>57</sup> A FOIA request can also trigger a reclassification or extension of classification, but requires a document-by-document review with the personal participation of, or under the direction of, the USD(I).<sup>58</sup>

### ***Controlled Unclassified Information***

CUI also need not be controlled indefinitely, although, unlike classified information, there are no specific dates at which the information is no longer protected.

CUI shall be decontrolled as soon as possible when it no longer requires safeguarding measures and dissemination controls pursuant to its associated authorities. CUI may not be controlled indefinitely unless law, regulation, or Government-wide policy so stipulates. CUI that has been publicly released via authorized agency procedures shall be considered decontrolled.<sup>59</sup>

### **Changing the Level of Classification**

Information can be downgraded to an appropriate level once the information no longer requires classification at the originally assigned level. It can also be upgraded by officials who have been delegated with the appropriate level of OCA. An OCA can change the level of classification as long as the information continues to meet the standards for classification. When the level is changed by the OCA with jurisdiction, the document(s) will be re-marked with the new classification level, the date of the action, and the authority for the change. Such a change may also result in new markings within the document, updates to the SCG, and notification to all known authorized holders of the information.<sup>60</sup>

A challenge can also be made to classification. In particular, if an authorized holder of information believes the information is improperly or unnecessarily classified, they can present that information to their ASM/CSM or the OCA. This can be completed through a formal

---

<sup>57</sup> DoD Manual 5200.01, *DoD Information Security Program: Overview, Classification, and Declassification*, Volume 1, Enclosure 4, pp. 44-45.

<sup>58</sup> *Ibid.*, p. 46.

<sup>59</sup> Guidance from NARA reference provided by Washington Headquarters Services (email 5/28/2013).

<sup>60</sup> DoD Manual, 5200.01, *DoD Information Security Program: Overview, Classification, and Declassification*, Volume I, Enclosure 4, p. 37.

challenge, but it is best to begin with informal questioning. Such a challenge may also arise in cultural resource work if it appears to the researcher that a certain document should have been declassified by a certain period, but it has not yet been released. It could also arise through a CRM with clearance, knowledge of the classification requirements, and a need to access the information. Each DoD Component will have procedures to challenge classification; however, until a determination is made, the information will retain its original classification status.

### **Unauthorized Disclosure**

Although the DoD has processes and protocols to prevent the release of classified or CUI to the public, on occasion this does occur. If information has been inadvertently released to the public it can still remain classified or, alternatively, the OCA may determine that it should be declassified. If the information should remain classified, the OCA will notify the known authorized holders of the information and provide marking guidance; the authorized holders should then take the appropriate actions to mark the material and apply controls.

*TIP: If your current or past project has resulted in an unauthorized disclosure. Do not contact those to whom the document was released; work with your ASM/CSM. Odds are that your security professionals will tell you to let it lie—pointing attention to the disclosure only creates an alert that classified or CUI is in the document.*

Information has also been known to be “declassified” by personnel without the proper authority to declassify. In such cases, although the information has been released, it actually remains classified by the OCA with jurisdiction. In such an instance, the OCA will determine whether the information can be removed from the public and the markings restored.

In any case, once there has been an unauthorized disclosure, DoD personnel “shall not publicly acknowledge the release of classified information and must be careful not to make any statement or comment that confirms the accuracy of or verifies

the information requiring protection.”<sup>61</sup> If in the past, your program has provided historic contexts, popular reports, or other products that included information that could be considered classified or CUI, there is no “putting the genie back in the bottle.” You cannot acknowledge that the release occurred, including to SHPO and other consulting parties; however, in future projects, you should ensure that a similar mistake does not happen. Now that you know such a release is a possibility, if you do not apply controls, you can be sanctioned or prosecuted.

---

<sup>61</sup> Ibid., p. 44.

## PLANNING AND EXECUTING YOUR PROJECT

Every deliverable that you produce as a CRM will require review prior to final publication or release to the public. If you are creating a classified document, it will also require the same review process to determine its status. The required review process in the DoD includes three elements: ASM/CSM, OPSEC Manager, and PA. The specifics on who reviews the work and the process for review vary by DoD Component (more detail is provided on this in the Document Review Practices section for each DoD Component). Regardless of the procedural specifics, your product will be reviewed: 1) by an ASM/CSM to ensure the military material will not jeopardize ongoing or future operations; 2) by an OPSEC Manager to ensure that elements of CI that could compromise strategic or tactical operations are not disseminated; and 3) by PA to ensure that dissemination of material is consistent with military missions and viewpoints. All three reviews are to take place at the lowest echelon possible: if you are at an installation, the review should take place at the installation; if you are at headquarters, the review should take place at that level. However, there are certain INFOSEC or PA topics that may still require review at a higher echelon, such as the DoD Component level or by DOPSR, regardless of the level at which you initiate the review.<sup>62</sup> In addition, your subject matter may also require an outside review by another agency. Once the document is returned to you, you will have to go through the chain of command at your echelon to release the product to the public.

For the purpose of integrating CRM duties with the safeguarding of military information this handbook divides the project process into four phases: 1) Conception and Initiation; 2) Definition and Planning; 3) Startup (Launch); and 4) Performance. During conception and initiation, you will have identified the need for a project and are determining whether it will be contracted and if there are information protection issues associated with the work. During Definition and Planning, you are working with your Contracting Officer, COR, and other information professionals to develop the scope, schedule, budget, and contracting mechanisms. You will also begin to work with your SHPO if there is a Section 106 undertaking. During Startup (Launch), you will be defining the project for the participants and consulting parties, as well as informing your information professionals that the project has begun. During Performance, you will be carrying out the work (if in-house) or tracking the progress, supporting your contractor, and working with the consulting parties to ensure the project is on schedule. Each of these phases is discussed in detail below, and the overall integration of a CRM project with the safeguarding procedures is shown in Figure 3.

---

<sup>62</sup> While this is true for ASM/CSM and PA reviews, OPSEC reviews will occur at your echelon, as the OPSEC Manager has a specific list of items that are important at that echelon—other echelons will not be aware of the specific echelon OPSEC list.

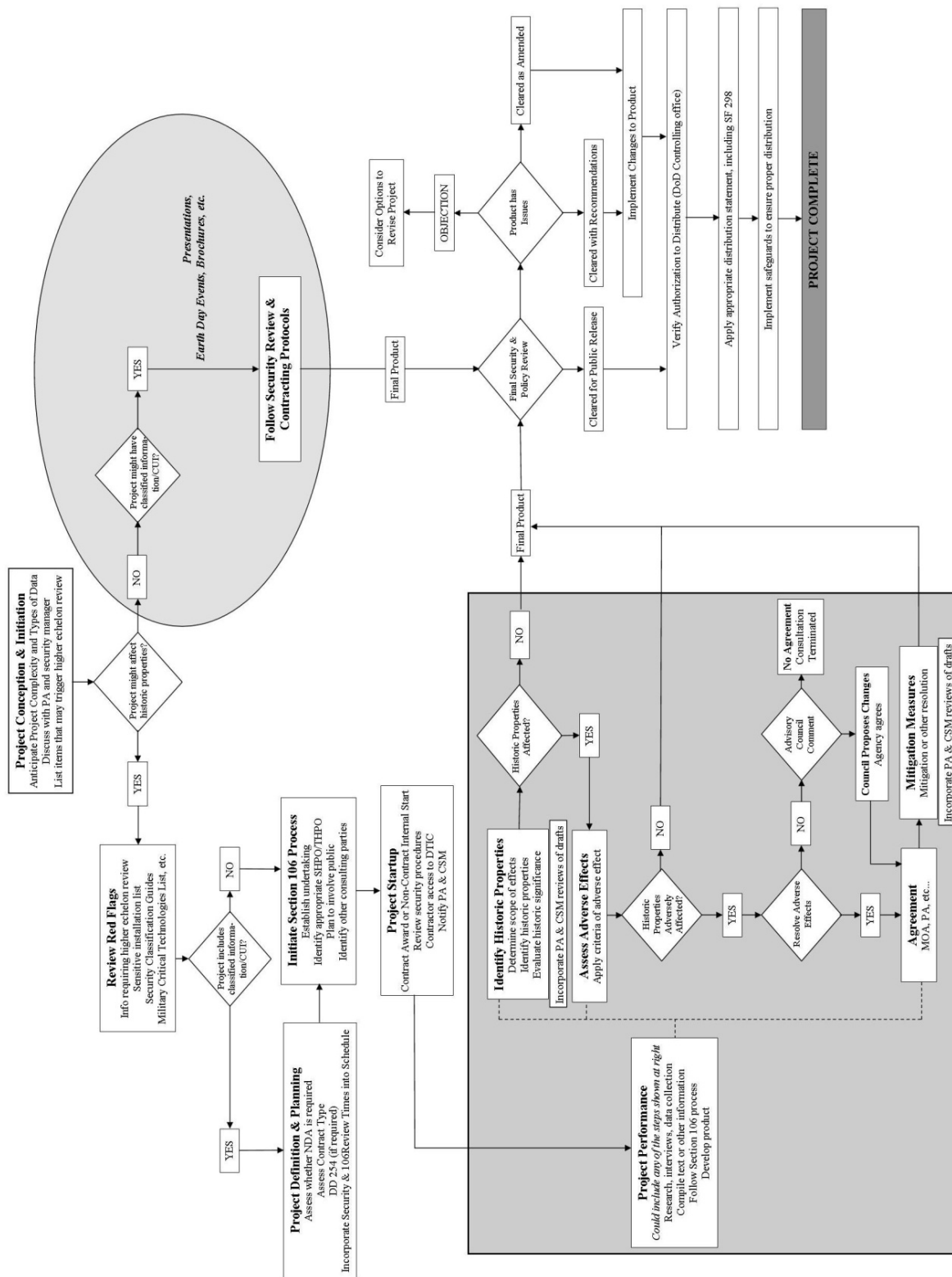


Figure 3. Section 106 and Safeguarding Information

When considering CRM and the National Historic Preservation Act of 1966, as amended, a basic question comes into play with regard to your SHPO and consultation: should the SHPO be considered the “public”? State agencies have a special standing with regard to information sharing; however, the Section 106 process is also designed to share information with the public. You should work with your organization and your INFOSEC, OPSEC, and PA staff to set up procedures that enable meaningful consultation while safeguarding classified information and CUI. This could be solved on a project-by-project basis or through a Programmatic Agreement for your program as a whole. You may want to include safeguarding in your Integrated Cultural Resource Management Plan as well. The appendices include an example non-disclosure agreement that you and your organization’s legal staff might use to aid in working with your SHPO with regard to certain military information you must share, but which should not be shared with the general public.

The following sections of the handbook are designed to aid you in determining as early as possible whether the subject matter of your study may require review at a higher echelon or with an outside agency. The level and intensity of the review process will directly affect your project budget and schedule and should be accounted for as early as possible. In order to do this you will need to proactively conduct some baseline research, be in contact with your ASM/CSM, OPSEC Manager, and PA, and, if your project is being contracted, the Contracting Officer that will be overseeing the contract with your consultant. In order to understand where the review may take you, you should first become familiar with the “red flag” items in this chapter—if your subject matter relates to one of the topics, it will require a more intensive review and may require a component, DOPSR, and / or outside agency review.

It is possible that you may find yourself in a situation where someone will not share information because they believe it is “sensitive” or was classified at one time. This person may be knowledgeable or not; the only way to know for sure is to refer to the respective SCG for that program, activity, or facility type. You are within DoD protocol to request a review of the information: you can call a meeting with your ASM/CSM and OPSEC staff to locate the applicable SCG and determine the actual status of a resource. When information is being withheld that does not merit protection, it is tantamount to creating “illegal secrets.” The best way to avoid perpetuating such illegal secrets is to request the SCG and / or a review to ensure you are indeed working with information that requires protection as required in DoD policy.

### **Phase I: Conception and Initiation**

At the outset of your project, you should consider the anticipated complexity and types of data that will be included to develop a review plan with a list of who should conduct the reviews, notification of those individuals about your project, and the proposed timing. It will be important to consider the ASM/CSM, OPSEC Manager, and PA reviews at the earliest stages of planning—whether the project is an historic context, documentation, historic survey or a Section

106 undertaking prescribed by a project proponent. As soon as you know that a building, site, test range, etc. is a component of the project you should assess the type of mission and military material that may be described in the course of the work. There are a number of steps you should take at this point to understand the content that may ultimately affect your review:

1. Assess the “red flag” issues provided in this chapter.
2. Conduct a search on the DTIC website of the SCGs that may apply. If there is an ASM/CSM assigned to your contract as COR, the COR will most likely conduct this research and advise you.<sup>63</sup>
3. Discuss the potential content with your ASM/CSM, OPSEC Manager, and PA.
4. Develop a list of items that will trigger review at a higher echelon, require a classified contract, or rethinking of the project (whether to include the classified topics); discuss with Contracting Officer if you know with whom you will be working.

*TIP: Use the “red flag” list in this document to identify whether you are working with a topic that is likely to require a more in-depth review process. Work with your PA, OPSEC Manager, and ASM/CSMs to develop project parameters and a schedule that incorporates the required review periods.*

Depending on your organization and echelon, the ASM/CSM, OPSEC Manager, and/or PA may not want to discuss the project until there is a product to review. However, it is important to reach out to them to gather as much data as possible to support the development of your scope so that at later phases you are not taken by surprise by long review periods, multiple agency involvement, or topics that would cause unanticipated security and policy issues. All of these could cause inordinate delays to your project schedule, stop-work orders, expensive contract modifications, or other unanticipated problems.

### Red Flag Issues

Below are types of information that may require review from a higher echelon, such as your DoD Component or DOPSR. If one of these is included in the product you are developing, you are likely to encounter the need for a review at more than one echelon and if an outside agency was the OCA, your product may also require a review by that agency. It is important to identify such red flags early in the development of a project, so you can anticipate the effects on your schedule and overall project.

#### ***Information that May Require Higher Echelon Review***

This does not include the comprehensive list, but rather a list of items that particularly applies to military CRM projects. If your research topic includes one or more of the following, it will

<sup>63</sup> This SCG index is only available to authorized government personnel and their contractors in the controlled access portion of DTIC at <https://www.dodtechopedia.mil/dodwiki/x/t4QiB>.



require a more intensive security and policy review and may be sent to a higher echelon, including DOPSR. It is also more likely that you may be running into information that is associated with OPSEC.

- Information on significant military operations
- Information on military applications in space
- Information on weapons and components of weapons of mass destruction (nuclear, biological, chemical)
- Arms treaty implementation
- Nuclear weapons effects research
- Chemical warfare and defensive biological / toxic research
- High-energy laser and particle beam technologies
- Nuclear, biological, and chemical defense testing and production, policies, programs, and activities
- National command authorities, command, control, communications, and intelligence
- Information, materials, and technical data on critical military technologies<sup>64</sup>

### ***Sensitive Installation List***

The list below itemizes topics that directly relate to installations and their historic missions, which could be considered classified or CUI.<sup>65</sup> The list is divided by DoD Component; if your project includes one or more of the following—keeping in mind that there may have been multiple uses in your project area—it is likely to require a more in-depth review. It may be sent to higher echelons (as high as DOPSR if the subject matter is on the list above) or require outside agency involvement.

#### **Army Installations**

- Nike surface-to-air missile batteries
- Safeguard antiballistic missile complexes (Spartan, Sprint interceptors)
- Nuclear weapons manufacturing / storage
- Chemical / biological weapons manufacturing / storage
- Essential communications sites

#### **Naval Installations**

- Naval facilities hosting submarine sound surveillance stations

<sup>64</sup> DoD Director of Administration and Management. DoD Instruction 5230.29, *Security and Policy Review of DoD Information for Public Release*, January 8, 2009, Enclosure 3, p. 6; Headquarters, Department of the Army. AR 360-1, *The Army Public Affairs Program*, May 25, 2011, p. 45-50; SECNAVINST 5720.44C, p. 2-8; and Secretary of the Air Force. AFI 35-102, *Public Affairs Security and Policy Review Process*, 20 October 2009, pp. 2-3.

<sup>65</sup> List compiled by SME advisors for this project.

- Naval Air Stations hosting Antisubmarine Warfare Operational Center / Tactical Support Centers
- Naval Air Stations hosting Advanced Undersea Weapon storage sites
- Nuclear weapons manufacturing/storage
- Essential communications sites

### **Air Force Installations**

- Airfields that hosted Strategic Air Command bombers and related facilities
- Airfields that hosted nuclear-equipped Air Defense Command fighter-interceptors
- BOMARC [Boeing and Michigan Aeronautical Research Center] surface-to-air missile sites
- ICBM [intercontinental ballistic missile] support bases (for Atlas, Titan, Minuteman, etc.)
- Nuclear weapons manufacturing/storage
- ICBM and SLBM [sea-launched ballistic missile] detection radars
- Satellite detection/tracking systems
- Air defense radars
- Air / space defense command, control, and communication nodes
- Essential communications sites (early warning, command-control, etc.)

### ***Critical Information List***

Consult your OPSEC Manager early in the planning process, and discuss the project with that manager. The manager will consult the CIL for your organization, which includes specific facts about military capabilities, activities, limitations and vulnerabilities that, if compromised, could allow adversaries to disrupt, degrade, or defeat a military mission. CI can either be classified or unclassified; that which is classified requires OPSEC measures for additional protection. CILs may contain unclassified, CUI, and classified portions, and you may be allowed to view the portion of the list for which you have clearance and appropriate need-to-know.

Any item in your proposed project that is on, refers to, or indicates aspects of elements on the CIL should be carefully considered. You should have a frank and thorough discussion about the relevance of information to the proposed project, and the need for this information, with the OPSEC Manager.

### **Other Resources**

In addition to the red flag items above—which will trigger a review at a higher echelon or an OPSEC review at your echelon—it will be important to be familiar with the resources listed below. They will provide more information about your subject matter and the type / levels of review your project may require. Your ASM/CSMs will be familiar with these resources and may know exactly which guides will apply to your project. It will be useful for you to become familiar with these resources and their typical content.

### *Security Classification Guides*

One way to avoid releasing classified data is to refer to the SCGs for the topics of your study—these can reveal which aspects of a given system, program, plan, etc. are sensitive and aid you in treating the information accordingly. SCGs, critical to the DoD ISP, are specific guides about military materiel and programs that detail how to classify and mark information related to the topic of a guide. You can use them to determine whether your project could potentially include information with which there may be classified information issues. The SCG addresses Critical Program Information—information about applications, capabilities, processes, and end-items; elements or components critical to a military system or network mission effectiveness; technology that would reduce the U.S. technological advantage if it came under foreign control; and other relevant information requiring protection, including export-controlled information and SBU information. These guides are developed in accordance with DoD Manual 5200.01, *DoD Information Security Program: Overview, Classification, and Declassification* and DoD 5200.1-H, *DoD Handbook for Writing Security Classification Guidance* and are reviewed and amended when necessary.<sup>66</sup>

SCGs are housed in the “DoD Techipedia” on the DTIC site as the “Security Classification Guide—Formerly Security Classification Guide Index.” This SCG index is only available to authorized government personnel and their contractors. The website includes a list of current and historical (cancelled or superseded) SCGs. They are listed by DoD Component, DoD Activities, as well as Joint DoD / DOE SCGs; and include hyperlinks to PDFs for most of the current SCGs. Historical SCGs are not available digitally on DTIC, though a list of these cancelled / superseded documents will list the OCA office that generated the SCG, and in some cases, a POC telephone number. These historical SCGs would be of interest to you, as it is likely that for a cultural resource project you and / or your contractor would be looking for information on military materiel that is associated with the older cancelled or superseded documents. However, it is likely that if the SCG is not in DTIC, you will not be able to access it.

A good starting point for using the SCG index on DTIC for project research is to consult the list of “Security Classification Guide Subject Matter Terms.” There are approximately 835 subject matter terms that can identify the main purpose of an SCG; these terms can be primary, secondary, or tertiary, and are more descriptive based on the number of terms used. An example of how to use this three level system is: FRUIT – APPLE – GRANNY SMITH. However, the terms are not required for inclusion in SCGs, are assigned by the author of a given SCG, and because they are not required, not all SCGs include these terms.

The lack of term consistency may make an initial comprehensive search difficult, yet, it will be important to browse the SCGs to determine whether any are quickly revealed that may affect

---

<sup>66</sup> DoD Manual, 5200.01, Volume I, *DoD Information Security Program: Overview, Classification, and Declassification*, Enclosure 6, pp. 69-73.

your project. Each SCG will identify specific items or elements of information to be protected and state the specific classification assigned to each item or element of information. Often, individual capabilities of systems are considered classified (range of a weapon, specific construction details of facilities used to test weapons) while others are not—the specifics are revealed in the SCGs. Once you have developed a general understanding of the SCGs and their applicability, make a list of general topics for further study and contact your ASM/CSM, OPSEC Manager, or PA—they should be able to direct you to applicable SCGs and assist you in streamlining your research or providing research information to your contractor (who should have SCG and DTIC access during the period of performance).

### ***Military Critical Technologies List***

The MCTL is a detailed and structured compendium of the technologies the DoD assesses as critical to maintaining superior U.S. military capabilities. The MCTL is used as a technical foundation for U.S. proposals for export control in the New Forum, Missile Technology Control Regime, Nuclear Suppliers Groups, Australia Group, and other nonproliferation regimes. The MCTL is used as a reference for evaluating potential technology transfers and technical reports and scientific papers for public release. The information is used to determine if the proposed transaction would result in transfer that would permit potential adversaries access to technologies, not whether a transfer should or should not be approved.<sup>67</sup>

If a resource you are studying appears on the MCTL, or is associated with it, your project will likely require: 1) an OPSEC review at your echelon and security and the required policy review(s) at higher echelons; 2) a DD 254 (Contract Security Classification Specifications)—regardless of contract classification status; and 3) the applicable SCGs for the project subject matter. During the course of work, if you require a document that should not be classified, you and your contractor should strive to not include detailed specifics about the materiel or missions. Referring to the SCG will help to avoid pitfalls, as they are clear about what types of information may be classified or CUI.

### ***International Traffic-in-Arms Regulations***

The ITAR is a series of DOS regulations driven by the Arms Export Control Act<sup>68</sup> that list technical data about arms and munitions prohibited from export. It includes any unclassified information that can be used, or be adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operations, maintenance, or reconstruction of arms, ammunition, and implements of war contained in the U.S. munitions list.

---

<sup>67</sup> <http://www.fas.org/irp/threat/mctl98-2/>

<sup>68</sup> U.S.C. Title 22—*Foreign Relations*, Chapter 39—*Arms Export Control*.

This list could include older weaponry that may be discussed in cultural resource documents. More information on the ITAR is available on the DOS website.<sup>69</sup>

In the planning phase of your project, you and your contractor should review the ITAR, specifically Part 121–The United States Munitions List. Any item on this list, which are called defense articles and services, may require special consideration and permission for export, and therefore any information about those items must be carefully handled. Particular attention should be paid to those articles deemed “Significant Military Equipment”<sup>70</sup> and to the articles and services described in the Missile Technology Control Regime Annex.<sup>71</sup> You should be familiar with this document, but be sure to check for updates to the ITAR, which are published every April 1<sup>st</sup> in the Federal Register. If your proposed project involves ITAR items, you should consult with your ASM/CSM, OPSEC Manager, and PA to seek their guidance. If you are already working with your Contracting Officer, you should discuss this with that person as well.

### ***Additional Information***

Final resources to consider in project planning include other reports and documents that involve similar topics. These documents can be found online on the DTIC website, on the Defense Environment, Safety and Occupational Health Network and Information Exchange (also known as DENIX— <http://www.denix.osd.mil/>), on the U.S. Army Corps of Engineers, Engineer Research and Development Center website (<http://www.erd.usace.army.mil/Library.aspx>), and in the libraries of the various military history offices. You should pay close attention to the distribution statements on these documents, especially if they are restricted in any way. For example, an FOUO report on a subject similar to the one you plan to research will give you an idea of what aspects may need special considerations. Also remember, however, that classified information may have been inadvertently included in publicly released documents / reports from some of the sources listed on these sites.

## **Phase II: Definition and Planning**

Once you have completed the project initiation phase, you will need to develop a full scope of work and anticipated schedule. If the work will be contracted you should also produce a government estimate. Whether the project is to be contracted or completed in house, if during project initiation you discovered that there will be classified, CUI, or other data

*TIP: Include in the scope of work the review requirements and specifications, including numbers of copies required, font sizes, review periods, etc. Work with your information professionals during early project planning to ensure you incorporate their requirements into the scope of work and have accurate information for the contract documents.*

<sup>69</sup> [http://pmdtc.state.gov/regulations\\_laws/itar\\_official.html](http://pmdtc.state.gov/regulations_laws/itar_official.html)

<sup>70</sup> This also includes technical data directly related to the manufacture or production of the articles.

<sup>71</sup> This list begins with paragraph 16 of Part 121 of U.S.C. Title 22–*Foreign Relations, Chapter 39–Arms Export Control*.

issues, you should refine the scope and schedule with your ASM/CSM, OPSEC Manager, and PA. Be sure to include as much information as you know at this point about the timing for local, higher echelon, and outside agency review.

## **Contracting**

Once you have determined what type(s) of information may be involved, you are now at what is known in the Federal contracting world as the “presolicitation phase” and you should provide your project information to the Contracting Officer, with a list of potential classified information issues / topics. The Contracting Officer will then develop the contracting for the project.

Once you have provided your project information to the Contracting Officer, they will review the proposed solicitation to determine whether access to classified information may be required by the contractor or subcontractor during contract performance, and, as such, whether the contract will be a classified contract. Under FAR, a classified contract is “Any contract that requires, or will require, access to classified information (Confidential, Secret, or Top Secret) by the contractor or its employees in the performance of the contract. A contract may be a classified contract even though the contract document itself is not classified.”<sup>72</sup>

During this process of assessing the contract type, the Contracting Officer will determine whether access to classified information of their agency or of another agency may be required. If access to classified information from the Contracting Officer agency is required, the Contracting Officer will follow NISP, and / or agency procedures, and include the FAR Security Requirements clause (52.204.2), which requires contractors to meet the security requirements of the NISP Manual. If access to classified data of an outside agency is required, the Contracting Officer will then determine if the agency is covered by the NISP and if they are, follow the agency procedures for determining the security clearances of firms to be solicited.

Once this background research is completed by the Contracting Officer, they will have defined whether the contract should be classified or not. Classified contracts require a DD Form 254. This form must be part of the contract package and is also used to identify other security requirements that the DoD Component may impose on a contractor. The DD 254 informs the contractor of the level of information they will be required to access; the level of security clearance the contractors will need; and how they will process, store, transmit, and destroy the classified information when the contract is complete. In addition, if the contractor then subcontracts the work, they are obligated to pass those requirements on to the subcontractor(s).<sup>73</sup>

---

<sup>72</sup>U.S. Government Printing Office. *Title 48 - Federal Acquisition Regulations System, Chapter 1 – Federal Acquisition Regulation, Subchapter H – Clauses and Forms, Part 52 Solicitation Provisions and Contract Clauses, Subpart 52.2 - Text of Provisions and Clauses, Section 52.204-2 - Security Requirements*, October 1, 2002.

<sup>73</sup> Ibid.

If classified information and a DD 254 are not required, but your project may incorporate unclassified but protected information, this should be evaluated to ensure that contractors have undergone an appropriate level of background investigation to perform the required duties. In addition, contractors must be made aware of any procedures or requirements regarding proper protection of unclassified information that merits such protection.

### **In-House CRM Projects**

In-house work that involves the public is a matter-of-fact for CRMs who work at the installation level. There are numerous CRM activities that may not include a contractor, but will involve sharing information with the public including Section 106 consultation, Section 110 surveys, tribal consultation, environmental assessment inputs, presentations to local groups, Earth Day activities, popular reports or brochures, tours, and other public outreach.

You should follow the same initial project steps that are discussed in the contracting section above when planning to complete a project or task in-house to determine whether classified information or CUI will be involved. Because there is no contract, you will not be working with a Contracting Officer; however, you should still contact your ASM/CSM, OPSEC Manager, and PA reviewers to discuss the work and determine the extent of reviews that will be required. You should meet with them early to discuss your role and their expectations—CRM is a highly specialized discipline that may be unknown to security and PA professionals, so be prepared to explain all that you do and how your work is tied into many different aspects of installation management. You should also ask the security / PA professionals to explain their roles and responsibilities and how they apply to CRM and installation operations. Finally, be sure to share copies of your local (if any) DoD Component and DoD policies for CRM, and ask them to provide the same. Under DoD policy, the process for security and PA—including document requirements and reviews—should be clearly defined and outlined in policies for your echelon.

Some of your in-house activities may be recurring events, for which you may want to meet with your reviewers to understand / establish the ground rules and then plan the activities using those rules. From time-to-time you should check back with reviewers to ensure there have been no policy changes that affect this ongoing activity. If you are producing a document in-house, you will need to follow the same document review protocol as you would if there were a contract. In short: if your information will be seen, heard, or read by the public, you are responsible to ensure it has had a proper security and policy review prior to releasing *any* information.

### **Special Considerations for Historical Researchers**

Regardless of how you implement your project, via a contract or in-house, you should know that there are additional approvals required for historical researchers to access **classified** archival or research materials. In addition to the FAR and contracting procedures, DoD Manual 5200.01 requires the DoD Component Head or senior agency approval to authorize access to classified

information for historical researchers. In order to obtain the authorization, the following are required:

1. A written determination that access to classified information is clearly consistent with the interests of national security and that the person requesting access has been found to be eligible for access.
2. A limitation on access to specific categories of information—within the scope of research—over which the DoD Component has classification jurisdiction. This can also include written consent of another DoD Component or non-DoD agency with classification jurisdiction over the specific categories of information required for the research project.
3. Authorization to access documents held by NARA or approval to access the classified material at a DoD installation or activity.
4. An agreement from the researcher to safeguard the information and to submit any notes and manuscripts intended for public release for review by all DoD Components or non-DoD departments or agencies that have classification jurisdiction in order to determine whether classified information is contained therein.
5. A written access authorization for no more than 2 years from the date of issuance. The DoD Component may renew access for 2-year periods in accordance with DoD Component issued regulations.<sup>74</sup>

*TIP: If you are unsure whether a product you are developing contains CUI or classified information, the **safest way to transmit the material for review is hard copy**. If you email a document to ask whether it has information that should be protected—and it does—you may have already compromised that information and government computer by using an unsecure channel for communication. This can also lead to the inconvenient process of having your computer scrubbed.*

### **Incorporating Reviews into a Project**

Whether you are completing your project through a contract or in-house, you will need to incorporate proper review times and anticipate the need for multiple echelons or outside agency review. Each echelon and agency will have its own standards for review periods, some will not accept draft documents, others require hard copies, and most have requirements on font size, etc. Be sure to familiarize yourself with these requirements and use them as you develop your product or, if contracted, include them in the contract documents. If you do not tell the contractor the specifications required for review, it is likely that your deliverable will not meet them and a contract modification may be needed to revise the product. Below are some of the details you will

<sup>74</sup> DoD Manual, 5200.01, *DoD Information Security Program: Protection of Classified Information*, Volume 3, Enclosure 2, p. 16-18.



need-to-know, but be sure to make yourself familiar with the specific requirements at your echelon and DoD component.

As a CRM you already incorporate the time it takes for consultation, review, comments from your SHPO and other consulting parties; however, you should also build in the anticipated time it will take for ASM/CSM, OPSEC Manager, and PA reviews into your project schedule. The time it will take for these reviews is wholly dependent upon the type of information with which you and your contractor will be working. At the outset of a project you may not be able to foresee new information that may arise; however, you should do the best you can to anticipate the issues that could result in extended / multi-level reviews in order to avoid delays on your project.

Typical ASM/CSM, OPSEC Manager, and PA reviews for each DoD Component are described in the following sections. If your project is to be reviewed by DOPSR, you will need to fill out a DD Form 1910, *Clearance Request for Public Release of Department of Defense Information*. It is a one page form that includes the document description, author, POC, prior coordination you may have completed, and submitting agency information. A copy of the current form is located in Appendix B of this document and online.<sup>75</sup> Below are the typical review periods associated with a DOPSR review:

1. Papers, articles, briefings and other similar material: 10-15 working days.
2. Technical papers and brochures: 15-20 working days.
3. Larger documents, such as manuscripts and reports: at least 30-60 working days (may take longer, depending on number of document pages / complexity).

### **Phase III: Startup (Launch)**

#### **Contracting**

This phase begins with the contract award. At that time the Contracting Officer will inform contractors and subcontractors of the security classifications and requirements assigned to the various documents, materials, tasks, subcontracts, and components of the classified contract.

This will follow the data on the DD 254, information that was developed specifically for contracts that include CUI, or other specific agency procedures (for those agencies that are not covered by NISP).

Once your project has gone through contracting, has been awarded, and a consultant is on board all project participants will be aware that the contract is classified, unclassified but includes information that should be safeguarded, or standard.

*TIP: Be sure to provide accurate and defined sources for your information--this will aid the reviewers in expediting your document. Tabbing or marking your document to show where information specific to that review is located is also helpful.*

<sup>75</sup> <http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd1910.pdf>. As with any document found online, check to ensure that you are using the most current version.

If the work is classified or includes protected information you should provide the contractor with access to DTIC so they can research SCGs and other project related material. You should also conduct a project startup meeting to review site access, security procedures, information safeguarding requirements, preparing drafts for security and policy review, scheduling, and other important issues that relate to completing the scope of work. You should also notify the ASM/CSM, OPSEC Manager, and PA that the project has started and the timing of anticipated products that will be ready for review. Although there are published review times, at certain times during the calendar year the reviewers are unavailable—if you plan for your review during one of those periods, your project will suffer delays. Working with your reviewers in advance to schedule reviews will help to streamline the project.

### **In-House CRM Projects**

As you begin the project, if there has been more than a short period since your initial discussion with your ASM/CSM, OPSEC Manager, and / or PA, you should meet with these reviewers

*TIP: Whether in-house or contracted, as the project progresses, be sure to keep your reviewers apprised of the schedule and when products will be available for review. Working with them in advance to schedule reviews will help to streamline your project.*

again to discuss the final scope, schedule, and anticipated public involvement / information release. During the meeting(s), you should work to define the security classifications and requirements assigned to the various documents, materials, tasks and components of the anticipated classified or CUI information that will be involved. You should also review site access, security procedures, information safeguarding requirements, and preparing drafts for review.

### **Phase IV: Performance** **Tracking the Project**

*TIP: You and your contractor should not include detailed, specific military materiel or mission capabilities. Use approximates to provide the information to describe historic importance. The words "about, approximately, near" can be helpful in avoiding a document returned for changes. Your reviewer may frown upon this, so it does not guarantee that it will not be returned; however it can be better not include such detail.*

You have begun the work or the contract has been awarded, the staff at your echelon is aware of the potential classified information review and schedule, and the contractor or your in-house staff has begun work. Now you will track project progress and assess whether there are any unforeseen classified data issues that may affect the schedule. Be sure to continue working with your ASM/CSM, OPSEC Manager, and PA to ensure timely reviews. Be sure to follow the process(es) noted for your DoD Component that are described in the following sections of this report.

Many ASM/CSM, OPSEC Managers, and PA will only review a final document. This will require at least one

additional layer of review and comment for your project. According to DoD policy, and DOPSR, there are five possible outcomes to a security and policy review:

- Cleared for Release
- Cleared, with Recommendation
- Cleared, as Amended
- Objection, Not Cleared
- Returned without Action

Be sure to follow the project process as noted for each DoD Component. Once the review / project is complete and approved for release to the public, you will need to incorporate a distribution statement and SF 298, Report Documentation Page.

## Distribution Statement

Once your project is complete and has gone through security and policy review, you will need to include a distribution statement. These statements are used in addition to classification and dissemination markings on documents to ensure there is not a secondary distribution beyond the intended primary distribution. Distribution statements are intended to allow for the maximum effectiveness of works that are not to be released to the public—those documents with statements B through F are to be treated to the same standard as FOUO and are subsequently to be destroyed using methods that prevent disclosure of the information. All records with a distribution statement are to be maintained in accordance with NARA requirements.<sup>76</sup> Distribution statements must be clearly displayed on the cover of the document, on the title page inside the document, as well as in the completed SF 298, which should be included in the final document to be released.

*TIP: Understanding Distribution Statements will help you to understand the constraints on information in a document, and will help in developing your document so that it can be available to the intended audience.*

### Statement Requirements

Below are the current distribution statements that are used for military work:

#### Distribution Statement A

Information is available to anyone. The actual statement language is: “Approved for public release; distribution is unlimited.” The statement can only be used on unclassified technical documents, cleared for release.<sup>77</sup> Most DoD documents that result from fundamental research

<sup>76</sup> Under Secretary of Defense for Acquisition, Technology and Logistics. DoD Instruction, Number 5230.24, *Distribution Statements on Technical Documents*, August 23, 2012, Enclosure 3, p. 13.

<sup>77</sup> The person who clears the document must be a competent authority in accordance with DA&M, DoD Directive 5230.09, *Clearance of DoD Information for Public Release*, August 22, 2008 (cleared through August 22, 2015) and DA&M, DoD Instruction 5230.29, *Security and Policy Review of DoD Information for Public Release*, January 8, 2009.

efforts are typically assigned the Distribution Statement A. However, if a document has a “likelihood of disclosing performance characteristics of military systems, or of manufacturing technologies that are unique and critical to Defense, and agreement on this situation has been recorded in the contract or grant” it will likely receive a different statement.

Generally, the technical documents with a Distribution Statement A are available to the public and foreign nationals, companies, governments, and they can be exported. However, the statement cannot be used for technical documents that were formerly classified—unless they have been cleared for public release. It is never used for classified technical documents or documents that contain export-controlled technical data.<sup>78</sup>

### **Distribution Statement B**

Information is available to U.S. government agencies only. The actual statement language is: “Distribution authorized to U.S. Government agencies only [include reason and date]. Other requests for this document shall be referred to the [include the controlling DoD office].” Both unclassified and classified technical documents can receive a Distribution Statement B. This statement is usually assigned when one or more of the following apply:

1. **Administrative or Operational Use:** typically applies to manuals, pamphlets, weapon system specifications, technical reports, and other publications with technical data.
2. **Contractor Performance Evaluation:** used to protect management reviews and records of contractor performance.
3. **Critical Technology:** used to protect information that could make a significant contribution to the military potential of any country.
4. **Export Controlled:** to protect unclassified technical data that is subject to DoD Directive 5230.25.
5. **Foreign Government Information:** used to protect and limit the distribution of information provided by foreign governments, as shown in the desires and agreements with those governments.
6. **OPSEC:** Used to protect information that could be observed by adversary intelligence systems to derive CI that may be useful to those adversaries.
7. **Premature Dissemination:** used to protect patentable information for systems that are in the concept state or the process of being developed.
8. **Proprietary Information:** Used to protect information not owned by the U.S. government.

---

<sup>78</sup> Under Secretary of Defense for Acquisition, Technology, and Logistics. DoD Instruction, 5230.24, *Distribution Statements on Technical Documents*, August 23, 2012, Enclosure 4, pp. 14-15.

9. Test and Evaluation: to protect results of military test and evaluation of commercial products when disclosure could cause an unfair advantage / disadvantage to the manufacturer.
10. Software Documentation: used to protect technical data that relates to computer software.
11. Specific Authority: used to protect information that is not specifically included in the instruction for distribution statements; if this is used, a specific reason must be stated.
12. Vulnerability Information: used to protect information and technical data that provides insight into DoD warfighting capabilities that are vital to national security.<sup>79</sup>

### **Distribution Statement C**

Information is available to U.S. government agencies and their contractors. The actual statement language is: “Distribution authorized to U.S. Government Agencies and their contractors [fill in reason and date of determination]. Other requests for this document shall be referred to [insert controlling DoD office].” This statement may be used for unclassified and classified technical documents. See Table 3 for the reasons that apply to Distribution Statement C.

### **Distribution Statement D**

Information is available to DoD Components and their contractors. The actual statement language is: “Distribution authorized to the Department of Defense and U.S. DoD contractors only [fill in reason and date of determination]. Other requests shall be referred to [insert controlling DoD office].” This statement may be used for unclassified and classified technical documents. See Table 3 for the reasons that apply to Distribution Statement D.

### **Distribution Statement E**

Information is available to DoD Components only. The actual statement language is: “Distribution authorized to DoD Components only [fill in reason and date of determination]. Other requests shall be referred to [insert controlling DoD office].” This statement may be used for unclassified and classified technical documents. In addition to the twelve reasons for assigned Distribution Statements B, C, and D, which also apply to Distribution Statement E—this also includes Direct Military Support. If this reason applies, the document will also contain “export-controlled technical data of such military significance that release for purposes other than direct support of DoD approved activities may jeopardize an important technological or operational military advantage of the United States.”<sup>80</sup>

<sup>79</sup> DoD Instruction, 5230.24, *Distribution Statements on Technical Documents*, Enclosure 4, pp. 15-17.

<sup>80</sup> DoD Instruction, 5230.24, *Distribution Statements on Technical Documents*, Enclosure 4, p. 19.

**Distribution Statement F**

This is the most restrictive statement. The actual language is: “Further dissemination only as directed by [inserting controlling DoD office and date of determination] or higher DoD authority.” Specific reasons in Table 3 do not generally apply to this distribution statement.

**Applying the Statement**

There are three steps to applying a distribution statement—all three relate to the contract between the government and contractor. First, the DoD controlling office must verify the government’s authorization to distribute. Second, the appropriate distribution statement should be applied, which is also reliant on the government rights as noted in the contract. And third, the agency should implement appropriate procedures and safeguards that govern the distribution of the product. The statement must be shown on the title page, front cover, and the SF 298, and it will be a standard distribution statement as noted in DoD Instruction 5230.24, *Distribution Statements on Technical Documents*. A copy of the current SF 298 used by the Government is located in Appendix B of this document.

**Table 3. Distribution Statement Types and Reasons**

	DISTRIBUTION STATEMENT	A	B	C	D	E	F
	Dissemination	Available	U.S. Gov’t Agencies Only	U.S. Gov’t Agencies & Contractors	DoD Components & Contractors	DoD Components Only	Limited by Controlling DoD Office
	Public Release	√					
	Administrative or Operational Use		√	√	√	√	
	Contractor Performance Evaluation		√			√	
	Critical Technology		√	√	√	√	
<b>R</b>	Export Controlled		√	√	√	√	
<b>E</b>	Foreign Government Information		√	√	√	√	
<b>A</b>	Operations Security		√			√	
<b>S</b>	Premature Dissemination		√			√	
<b>O</b>	Proprietary Information		√			√	
<b>N</b>	Test and Evaluation		√			√	
	Software Documentation		√	√	√	√	
	Specific Authority		√	√	√	√	
	Vulnerability Information		√	√	√	√	
	Direct Military Support					√	

# DEPARTMENT OF THE ARMY DOCUMENT REVIEW PRACTICES

All current and former Army personnel have a **lifelong obligation** to protect classified information and controlled unclassified information, and to follow established procedures to obtain security reviews of articles, books and other media prior to public release.

Principal Deputy Chief of Public Affairs, May 2011

## **Purpose**

The U.S. Army is responsible for the classification and safeguarding of information that requires protection in the interests of national security, including classified information, CUI, FOUO, and SBU information, as well as safeguarding of RD and FRD. The DoD requires that any official information intended for public release which pertains to military matters, NSI, or subjects of significant concern to the DoD must be cleared by the appropriate OPSEC, CSM, and PA offices prior to release—this also includes materials that are to be placed on the Internet or released via similar electronic media. It is the duty of all Army personnel/employees and their contractors, licensees, certificate holders, and grantees to protect the above information against unauthorized disclosure. Each individual associated with the Army has a personal, individual, and official responsibility for the proper safeguarding and protection of the information to which they have access.<sup>81</sup>

## **Roles & Responsibilities**

It is Army policy that there will be OPSEC, CSM, and PA reviews prior to the release of information to the public. As the CRM, it is important for you to be involved in the protection of classified information and CUI.<sup>82</sup> There are many other individuals in your chain of command who have specific responsibilities; however, you—as the communicator or project originator—have a responsibility to be aware of Army policies and protect the information. Whether you are involved in a cultural resource deliverable, a media interview, giving a speech, posting something on the Internet, or communicating in other electronic or verbal means (for work or at home)—you are responsible for protecting classified information from unauthorized disclosure.

It is the responsibility of PA to work closely with their local engineers and environmental coordinators on a continuing basis. The Army is charged with complying with Federal, State and

<sup>81</sup> U.S. Army Public Affairs, AR 360-1, *The Public Affairs Program*, 25 May 2011, p. 4.

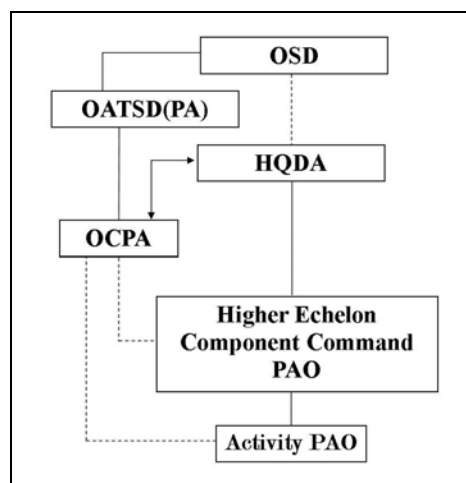
<sup>82</sup> Security of classified data also extends to visitors—personnel without DoD clearance are not allowed access to spaces that have classified information. If they are to visit, all classified information must be covered to sanitize the area prior to their entry.

local environmental standards and demonstrating leadership in environmental enhancement— CRM work falls under this mandate. Your PA should work closely with you to ensure information that should be safeguarded is not released to the public during the process of meeting these legal requirements.<sup>83</sup>

This section on roles and responsibilities is designed to aid you in understanding the chain of command: where there are people who can help you to better understand classified information and CUI; when information will have to be sent to echelons above your activity for a review; and your place in the echelons with regard to safeguarding information. The primary review in the Army occurs within the spheres of OPSEC and PA. The classification and declassification of material occurs under the security program.<sup>84</sup>

### Public Affairs Program

Due to the sensitivity and the potential time criticality of incidents / issues with PA implications, Army PAOs require direct access to the commander. As such, PA is a command responsibility and PAOs serve on the commander’s personal staff. The primary PA functional areas are internal information, public information, and community engagement.



The Army encourages and authorizes the public release of information at the lowest level of responsibility; however, there are instances when a higher echelon review is required or when there is a question on the release authority. In those cases, your release material will be reviewed at a higher level and may be sent to the Office of the Chief of Public Affairs (OCPA).<sup>85</sup>

**Figure 4. U.S. Army, Public Affairs Program Organizational Chart**

Source: Derived from AR 360-1 text

**Headquarters, Department of the Army:** In accordance with AR 360-1, principal Headquarters, Department of the Army (HQDA) officials will prepare information, records, and material for the OCPA’s dissemination to the public. And, the OCPA staff officers will ensure that all necessary staff coordination and clearances have been completed prior to releasing information outside the Department of the Army.

<sup>83</sup> U.S. Army Public Affairs. AR 360-1, *The Public Affairs Program*, 25 May 2011, p. 39.

<sup>84</sup> U.S. Army Security. AR 380-5, *Department of the Army Information Security Program*, 29 September 2000, p. 15.

<sup>85</sup> AR 360-1, *The Public Affairs Program*, p. 1.



Within HQDA:

1. The OCPA has authority to release information about the Army as a whole. Such information is normally obtained from the Army Staff (ARSTAF) agency having primary interest and is cleared, as necessary, with the Office of the Secretary of Defense (OSD). ARSTAF agencies with technical liaison officers or PAOs may respond directly to requests for routine information.
2. The OCPA coordinates with the Office of the Chief of Legislative Liaison (OCLL), other DA staff agencies as appropriate, and the OATSD(PA) prepares all replies to congressional inquiries, requests, or other transmittals of information which may have significant PA implications prior to such information being forwarded to Congress by OCLL.<sup>86</sup>

**OCPA:** OCPA is authorized to communicate directly with other HQDA agencies, Army Commands (ACOMs) and installations, and subordinate Army elements, if attempts to contact the unit's and / or installation's higher headquarters in a timely manner have failed. In addition, commands and installations are authorized to communicate directly with the OCPA when circumstances require, after they have made reasonable attempts to contact their higher headquarters first. Any headquarters bypassed as a result of a direct communication will be informed of the action as soon as possible by the office initiating the direct communication.

The OCPA is organized into a HQDA element at the Pentagon and several field operating agencies. Below are the areas of interest for each of these PA organizations that may affect CRM:

1. Entertainment, television, and motion picture industries: OCPA, Los Angeles branch.
2. Broadcast, print, publishing, advertising, theatrical, and independent creative communities: OCPA, New York branch.
3. PA doctrine, training, leader development, organization, materiel, and Soldier and/or civilian support issues: Army Public Affairs Center.
4. Regional branch offices—as directed by the Chief, Public Affairs—provide liaison and support to the Army, other Service, and local ACOMs throughout the continental U.S.<sup>87</sup>

**Commands below HQDA level:** Release materials that are not under direct HQDA or OCPA purview can be released by commanders below HQDA level—as long as the information is wholly within the mission and scope of their commands. Such information should be submitted to the appropriate PAO who will prepare material for release and ensure a security review is conducted. The PAO either will grant clearance or forward the information to the appropriate headquarters for clearance.

<sup>86</sup> Ibid., p. 8.

<sup>87</sup> Ibid., pp. 1-2.

Whenever the DoD is supporting other Federal agencies—such as the Federal Emergency Management Agency, the Federal Bureau of Investigation, or the Department of Interior—PAOs will use the operational chain of command to coordinate visits, media opportunities, and information release. In addition, when there is a possibility of releasing military intelligence and security related information, photographs and video, and audiotapes must be authorized by U.S. Army Intelligence and Security Command.<sup>88</sup>

While CRM release materials may be affected by the above, the most likely area for CRM reports, as defined in AR 360-1, is that which affects “scientific studies.” The Army will review and clear materials proposed for release to the public by contractors, manufacturers, scientific researchers, and other entities regarding contractual agreements and awards, products, services, military sales, technology, scientific studies, and other areas of production and research. It is Army policy to make the maximum, accurate information available to the public about Army contractual relationships, industry accomplishments, and scientific achievements. The exceptions include:

1. Safeguarded information.
2. Data that offers unfair and competitive advantages to specific entities and individuals.
3. Non-exportable commercial information or data and information subject to ITAR.
4. Material that contains implied Army endorsement of a commercial firm, product, or service.
5. Comparison of the merits of one item of military material with another.
6. DoD specification details or results of acceptance tests.
7. Information involving critical military technology.<sup>89</sup>

Except for materials developed under contract requirements, PAOs act only in an advisory role to review material that is voluntarily submitted. If your contractor does not have a DD 254 associated with the contract, the deliverable should be voluntarily submitted to the PAO designated by the Contracting Officer. If you submit the document to another PAO, the PAO will send it to the administrative Contracting Officer for referral to the proper PAO. The final decision on matters of accuracy, style, and good taste of the deliverable remains with the originator—your PAO will only comment on information that should be safeguarded. PAOs do not have the authority to clear scientific and technical information for public release. However,

---

<sup>88</sup> Ibid., pp. 15-16.

<sup>89</sup> Ibid., p. 24.

PAOs will assist the proponent of unclassified scientific and technical materials in determining at what level clearance can be granted.<sup>90</sup>

## Operational Security Program

The Army OPSEC process identifies the CI for military plans, operations, and supporting activities and the indicators that can reveal it. OPSEC Managers then develop measures to eliminate, reduce, or conceal those indicators. The OPSEC process:

1. Identifies those actions that can be observed by intelligence systems of U.S. adversaries.
2. Determines indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive CI in time to be useful to U.S. adversaries.
3. Selects and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to exploitation by U.S. adversaries.<sup>91</sup>

OPSEC is the responsibility of all Army personnel and contractors. Failure to properly implement OPSEC measures can result in serious injury or death to military personnel, damage to weapons systems, equipment and facilities, loss of sensitive technologies, and mission failure. OPSEC is a continuous process and an inherent part of military culture, and as such, must be fully integrated into the execution of all Army operations and supporting activities. The following lists the primary roles and responsibilities that relate to CRM.

**Deputy Chief of Staff:** The Deputy is responsible for designating a full-time HQDA OPSEC Program Manager to establish Army OPSEC objectives, policies, and procedures. The Deputy coordinates the Army program with the Joint Staff, other military departments, and DoD, as well as providing guidance to the appointed HQDA Staff OPSEC Program Manager.

**HQDA Staff OPSEC Program Manager:** The HQDA Staff OPSEC Program Manager develops and implements a functioning, active, and documented OPSEC program to ensure the staff organization plans, integrates, and implements OPSEC measures to protect CI in every phase of all initiatives, programs, operations, exercises, tests, or activities.

**OCPA:** In addition to the PA program, the OCPA provides assistance to the HQDA Staff OPSEC Program Manager to increase OPSEC awareness throughout the Army.

**Commanders:** Commanders at all levels are responsible for ensuring that their units, activities, or installations plan, integrate, and implement OPSEC measures to protect their command's CI in every phase of all operations, exercises, tests, or activities. These commanders also have the responsibility to:

---

<sup>90</sup> Ibid., pp. 72-73.

<sup>91</sup> U.S. Army Operations and Signal Security. *Operations Security*, 19 April 2007, p. 1.

1. Appoint an OPSEC officer in writing, and ensure that officer receives the appropriate training. As a CRM at the installation / activity level, you should seek out this officer to answer any OPSEC questions you may have.
2. Establish an OPSEC Program, and an OPSEC Standard Operating Procedure (SOP). You should obtain a copy of this SOP, and use it as a guide to accomplish OPSEC reviews.
3. Approve the unit, activity, or installation CIL. You should obtain a copy of the CIL during your project planning phase to see if your project involves any of the included elements of information.

**Garrison Commanders:** In addition to the above requirements for commanders, Garrison Commanders are also responsible for developing an installation-level OPSEC working group to coordinate OPSEC actions among the tenant organizations and provide OPSEC guidance to them. An installation-level OPSEC working group can include, but is not limited to, tenant organization OPSEC officers, PAOs, CSMs, anti-terrorism/force protection officers, provost marshal office, Directorate of Information Management, and so forth. If you are a CRM operating at the garrison level, you should seek out the OPSEC working group in advance of your project planning phase to seek guidance on OPSEC requirements.

### **Information Security Program**

The Army ISP is responsible for the classification, downgrading, declassification, transmission, transportation, and safeguarding of information requiring protection in the interests of national security. It primarily pertains to classified NSI, now known as classified information, but also addresses CUI, including FOUO, and SBU—basically all information that is included under EO 13526.<sup>92</sup>

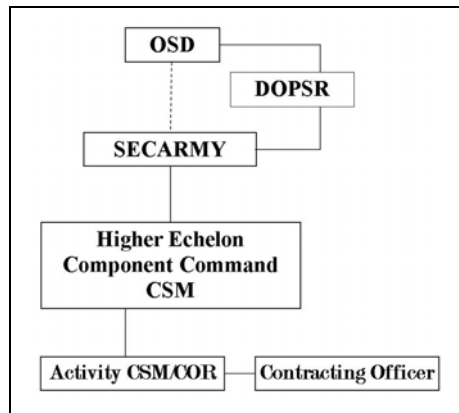
**The Secretary of the Army:** It is the responsibility of the Secretary of the Army (SECARMY) to appoint a senior agency official to direct and administer the ISP within the Army. The SECARMY will also commit the necessary resources for the effective implementation of the program and establish procedures to ensure that the head of each Major Command—that creates, handles, or stores classified and sensitive information—appoints an official to serve as CSM for the command. The SECARMY is the only Army official that may delegate TOP SECRET OCA.

**HQDA, Deputy Chief of Staff for Intelligence:** The Deputy is designated as the Army Senior Official of the Intelligence Community, to direct, administer, and oversee the Army's ISP. The Chief of the Counterintelligence / Human Intelligence Division, Intelligence Policy Directorate, provides staff support for these functions. This official ensures the promulgation of policy, procedures, and programs necessary for the implementation of EO 13526 and DoD Directives; ensures Major Command, Major Subordinate Commands, and other agencies review and assess

---

<sup>92</sup> U.S. Army Security, AR 380-5, *Department of the Army Information Security Program*, 29 September 2000, p. 1.

their classified and sensitive products; responds to INFOSEC matters pertaining to classified information and CUI that originated in an ACOM *that no longer exists* and for which there is no successor in function; and delegates SECRET and CONFIDENTIAL OCA to other Army officials.<sup>93</sup>



**The Commander:** In the Army, security is a command function and commanders, Officers in Charge, and heads of agencies and activities, are responsible to effectively manage their command ISP(s). Commanders may delegate the authority to execute the requirements of AR 380-5, but not the responsibility to do so. Security—including the safeguarding of classified information and CUI, as well as the appropriate classification and declassification of information created by command personnel—is the responsibility of the commander.

Figure 5. U.S. Army, CSM Organizational Chart

**CSM:** The CSM is the principal advisor on INFOSEC in the command and is responsible directly to the commander for management of the program. The CSM advises and represents the commander on matters related to the classification, downgrading, declassification, and safeguarding of NSI. In addition to other responsibilities, the CSM in your echelon will:

1. Establish procedures for access to classified information.
2. Be the single POC to resolve classification issues.
3. Review all classified and CUI documents and continually reduce, by declassification, destruction, or retirement, unneeded classified and sensitive material.
4. Establish and maintain visitor control procedures in cases where visitors are authorized access to classified information.
5. Ensure proposed public releases on classified and CUI programs be reviewed to preclude the release of classified information or other CUI covered under the FOIA exemptions.<sup>94</sup>

In addition to the CSM, your supervisor and you both have the responsibility to safeguard information. Although the Contracting Officer is not directly addressed in AR 380-5, under the FARs the Contracting Officer has great responsibility to ensure protected data is not released in the products that are developed under the Contracting Officer's contract.

<sup>93</sup> Ibid., p. 1.

<sup>94</sup> Ibid., pp. 2-3.

## **Geospatial-Intelligence**

In general, if you are working with your GIS group at your echelon, they will know whether your project is encroaching upon an NGA issue. However, if you or your contractor adds information to your maps, such as historical missions, building names, uses, training areas, ranges, etc. you may be compiling (aggregating) information that should be protected. The maps you create may be subject to NGA review or oversight. If your PAO or CSM has questions about such imagery, it will move to a higher echelon and may be forwarded to NGA for review.

## **Process**

It is Army policy that information will be released as expeditiously as practical and from the lowest possible echelon that is consistent with Army release policies and required reviews. As noted above, for cultural resource projects you may require both a PAO and CSM review.

As the CRM you will be responsible to oversee the work of your contractor and you may serve as the contracting officer's representative (COR). To support the contractor and the Contracting Officer, you should be familiar with the issues of classified data and conduct some initial project research to determine whether classified information or CUI could be an issue on the contract. If classified information was not identified at the outset of the project, as soon as you think there may be an issue, it is important to inform your Contracting Officer, the PAO, and CSM to coordinate items that may affect the contract and to develop a plan for review. The earlier your PAO and CSM know that you may be forwarding a project, the more likely it is that your deliverable will fit well into their schedule and be reviewed quickly.

Certain types of information will require that your deliverable move to a higher echelon or possibly to SECARMY, OCPA, or DOPSR. If your project does not include "red flag" topics, your review can occur entirely within your activity. However, depending on the information in your document, your CSM or PAO may still request the review from a higher echelon within the DoD or another agency within or outside the DoD. The request for another agency review will occur if your deliverable includes data from that agency and the CSM or PAO has identified them as the originator. They may also send the deliverable up the chain of command if there is a question about the sensitivity of the data.

Generally this conversation and transfer of the product occurs from PAO to PAO and from CSM to CSM. Also, your security review should be completed prior to forwarding your information to your PAO. On the PAO side, the highest the product is likely to go is OCPA, although OCPA may forward it to DOPSR, if it seems necessary. On the CSM side, your deliverable can move to SECARMY, who also may forward it to DOPSR. Unless the classified data issues are fairly easy to resolve, these two echelons will likely work together and pass the deliverable back and forth to ensure all issues have been reviewed thoroughly. If they feel the document requires additional subject matter expert (SME) review, it will be sent back to your higher echelon CRM

for review. Once that is completed, it will then be passed back to SECARMY. Also, as with other levels in the chain of command and PA, it may also be sent out for other agency review. After the review is completed, your document could be sent back to you with an approval or recommendations from whichever entity originally received the deliverable (Figure 6).

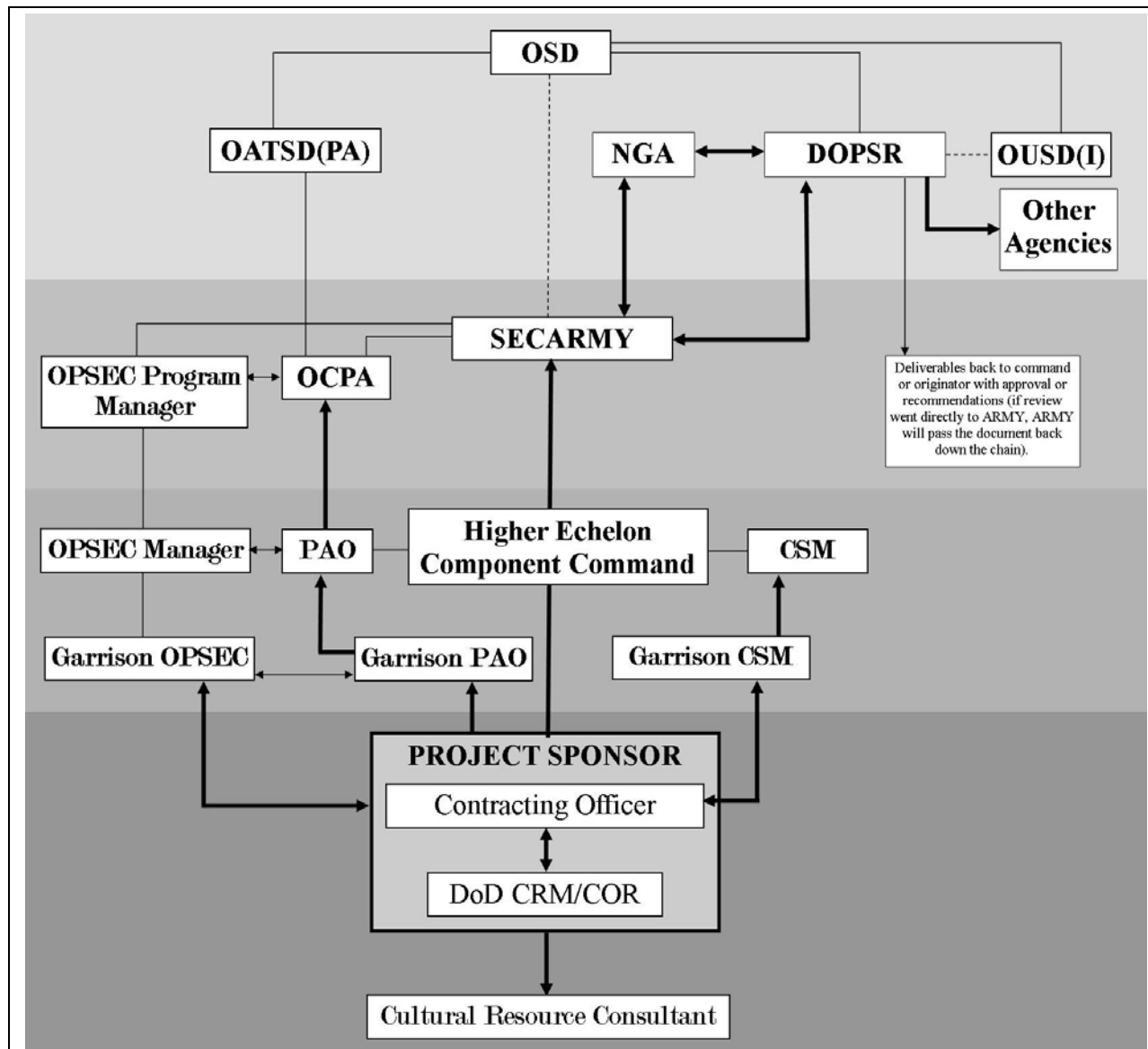


Figure 6. U.S. Army, Simplified CRM Security and Policy Review Chart

### Basic Review Times

The best way to streamline your review is to communicate early with your PAO and CSM so they know the basic precepts of your project and generally when your submittal will be coming to them for review. Below are the approximate review times, based on a DOPSR review. You should check with your ASM/CSM, OPSEC Manager, and PA to obtain the review times

required at your echelon. You may also want to build more time in your schedule if you believe your submittal will be moving up the chain of command a higher echelon or an outside review.

**Presentations/Speeches:** Submit speeches and briefings at least 5 working days before the event at which they are to be presented. Additional time may be needed for complex or potentially controversial speeches due to coordination requirements.

**Papers and Articles:** Submit at least 10 working days before the date that you need the review to be completed. The length, complexity, and content will determine the number of agencies that may be required to review the document and, consequently, the ultimate time required for the complete review process.

**Technical Papers/Reports:** Submit at least 15 working days before the date that you need the review to be completed. This is likely where the bulk of CRM work would fall; again, be sure to work with the local reviewers to understand whether there may be multiple reviews within the SECARMY, whether other DoD agencies may be required to review, and whether it may require review outside the DoD.

**Manuscripts and books:** Submit at least 30 working days before the date that you need the review to be completed. More time may be needed if the material is complex or requires review by other agencies. It is likely that such publications will require SECARMY or DOPSR review.

### **Submittals**

All information submitted for review should be coordinated within the originating DoD Component to ensure that it reflects the organization's policy position. As noted above, the submittal should be reviewed by PAOs and CSMs at the lowest echelon and only be sent further up the command chain if it is necessary. Only the full and final text of material proposed for release shall be submitted for review at the DOPSR level. This higher echelon will return draft or incomplete documents without action.

However, as noted above, at an earlier point in your project you may want to consult with your local PAO or CSM using notes, outlines, briefing charts, etc. to know whether your project may be headed for a higher review.

### ***Contractor Submittals***

The contract between the Army and your cultural resource contractor may include specific language about the procedures for submission, review, and clearance of industry-originated information materials. In such a case, your Contracting Officer will refer to Army/industry interface guidance in the FAR, Army FAR Supplement (known as AFARS), and Defense



Acquisition Regulations System (known as DFARS) and the relationship that is laid out in the contract terms.

A classified contract is one which requires access to classified information, either to submit a bid or proposal or to perform the contract. A contract may be classified even though the contract document is not classified. When a classified contract exists, the contractor is guided by security items in the contract and by the terms of the security agreement. The security criteria will be shown on DD Form 254. DoD 5220.22–R, DoD 5220.22–M, and AR 380–49 contain the procedures to safeguard classified defense information and procedures for the proposed release of information which contractors, subcontractors, vendors, or suppliers will have access to or possess.

When unclassified contracts do not provide specific instructions on the release of information, your contractor should submit review materials, prior to publication, to a PA office designated by the administrative Contracting Officer. If the submission is made to an office that is other than the one specified, it will be referred immediately to the proper administrative Contracting Officer for action. Voluntary submission is simple business courtesy and affords safeguards against accidental release of inaccurate, CUI, or classified information.

### ***Review Materials***

When submitting materials for review, you should coordinate the requirements and schedule with your PAO or CSM. At the time of this publication, the Army required at least three copies of each of the following:

1. Written materials and properly captioned still photographs. You must include an additional copy of all materials for each of the intervening HQDA record file.
2. Scientific and technical papers and presentations, including properly captioned copies of all viewgraphs, photographs, charts, graphs, and similar material.
3. Fact sheets, pamphlets, and brochures, including full text, layout, and all illustrative material.
4. Contractor advertisements—submit three copies. Each copy will include text and layout, including artwork and photographs, proposed for final publication.
5. Exhibits—submit three copies. Design/layout with text of copy to appear on display material and all artwork and photographs proposed for exhibition.
6. For motion picture or videotape production, the following review procedures are required:
  - a. Preliminary written story/concept/outline treatment—three copies. Include additional copies, one each for intervening HQDA record files.
  - b. Final shooting script, including scene description/narration—submit three copies. Include additional copies, one for each intervening HQDA record file.

- i. One copy rough cut (film or videotape) minus soundtrack.
- ii. One print (film or videotape) or one copy final narration for final review.

**Paper Submittals:** A minimum of three hard copies and a signed DD Form 1910, *Clearance Request for Public Release of Department of Defense Information*, to the:

Chief, Defense Office of Prepublication and Security Review  
Department of Defense  
Defense Office of Prepublication and Security Review  
1155 Defense Pentagon  
Washington DC 20301-1155

OR

Department of the Army  
ATTN: Chief of Public Affairs  
1500 Army Pentagon  
Washington, DC 20310-1500

**Electronic Submittals:** One copy in Microsoft Word with a signed DD Form 1910, by e-mail to:

[whs.pentagon.esd.mbx.secrev@mail.mil](mailto:whs.pentagon.esd.mbx.secrev@mail.mil) (Unclassified information only)

**Abstracts, Papers, and Presentations:** Abstracts that are to be published in advance of a completed document require clearance. Such clearance does not fulfill the requirement to submit the full text for review prior to its presentation or publication. If an abstract has been cleared in advance, the previous clearance and attached case number needs to be noted on the DD Form 1910 or other transmittal when the full text is submitted.

**Websites:** Information intended for placement on websites, or other publicly accessible computer servers, which are available to anyone, without access controls, may require review and clearance for public release. Your website clearance questions should be directed to your component's website manager.

### **Possible Outcomes**

**Cleared:** Information may be released to the public without restriction.

**Cleared as Amended:** Amendments are mandatory due to deletions or additions—DoD clearance is contingent upon the implementation of the noted amendments. The information may be released without restriction upon implementation of the amendments.

**Recommended Changes:** These are non-binding suggested changes to clarify or amplify information in the document.

**Not Cleared:** The information is not cleared and may not be publicly released.

**Returned Without Action:** This occurs when the reviewer is unable to review due to insufficient time, the material is already in the public domain, or the review may be cancelled upon request of submitter.

Intentionally Blank

# DEPARTMENT OF THE NAVY DOCUMENT REVIEW PRACTICES

## **Purpose**

The U.S. Navy and USMC<sup>95</sup> leaders are responsible for providing timely and accurate information to the public about their component activities. DoD Component information shall be made fully and readily available, unless its disclosure would adversely affect national security, threaten the safety or privacy of U.S. Government personnel or their families, violate the privacy of the citizens of the U.S., or be contrary to law. The obligation to provide the public with information may require detailed PAO planning, coordination within the DoD and coordination with the other government agencies. Planning with other services and agencies is to expedite the flow of information to the public.<sup>96</sup>

## **Roles & Responsibilities**

It is DON policy that there will be “Security at the Source,” i.e., the security of classified information and material is the responsibility of every individual within the DON. As the CRM, it is important for you to be involved in the protection of CUI and classified information, which is paramount when preparing information for public release.<sup>97</sup> There are many other individuals in your chain of command that have specific responsibilities; however, you—as the project originator—have a responsibility to be aware of DON policies and protect the information that should be safeguarded. Whether you are involved in a cultural resource deliverable, a media interview, giving a speech, posting something on the Internet, or communicating in other electronic or verbal means (for work or at home)—you are responsible for protecting classified information from unauthorized disclosure.

Under the DON ISP, military and civilian personnel are subject to criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of SECNAV Manual 5510.36, *Personnel Security Program* (summarized herein). In addition, military personnel are also subject to disciplinary action under the Uniform Code of Military Justice.<sup>98</sup>

---

<sup>95</sup> Collectively known as the Department of the Navy or DON.

<sup>96</sup> Department of the Navy. SECNAVINST, 5720.44C, *Department of the Navy Public Affairs Policy and Regulations*, 21 February 2012, pp. 1-2 through 1-4.

<sup>97</sup> Security of classified data also extends to visitors—people without DoD clearance are not allowed access to spaces which have classified information. If they are to visit, all classified information must be covered to sanitize the area prior to their entry.

<sup>98</sup> Department of the Navy. SECNAV M-5510.36, *Personnel Security Program*, June 2006, p. 1-1.

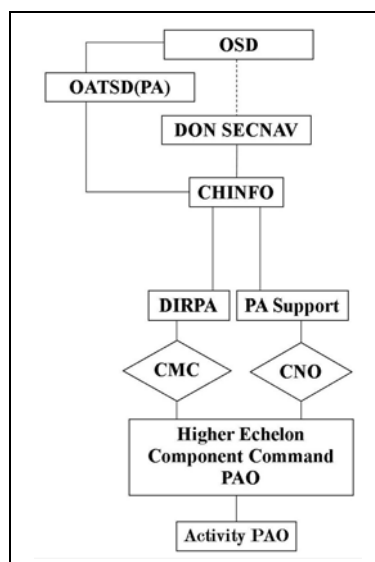
This section on roles and responsibilities is designed to aid you in understanding the chain of command: where there are people who can help you to better understand classified information and CUI; when information will have to be sent to echelons above your activity for a review; and how you fit into the overall chain of command with regard to safeguarding data. Within the DON there are three tracks of the review: CSM, OPSEC Manager, and PAO.

## Public Affairs Office

### Public Affairs

As noted above, it is the responsibility of the PAO to ensure that information is made fully and readily available—consistent with statutory requirements—unless its release is precluded by national security constraints or valid statutory mandates or exceptions. The charts and accompanying text below identify the major players within the PAO chain of command, as well as their primary responsibilities (see Figure 7).

**DON SECNAV:** SECNAV is responsible for establishing PA policy and directing its implementation. SECNAV monitors and controls U.S. Navy and USMC relations with the Congress, OSD, other principal government officials, and the public. Implementation of SECNAV policies is the responsibility of the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and other senior commanders who report directly to the Secretary.



**U.S. Navy, Chief of Information & USMC, Director of PA:** U.S. Navy, Chief of Information (CHINFO) reports to SECNAV and coordinates with the OASD (PA). The CHINFO acts as the public spokesperson for the U.S. Navy in coordination with the USMC, Director of PA (DIRPA)<sup>99</sup> and advises SECNAV and CNO on matters of policy, the public’s understanding of the U.S. Navy and USMC team, methods of information dissemination, and means to increase public awareness. The CHINFO also coordinates, evaluates, and forwards to the OATSD(PA) all DON information of national or international interest that is being considered for public release.<sup>100</sup>

Figure 7. U.S. Navy, Public Affairs Office Organization Chart

**CNO and CMC:** The CNO and CMC—the U.S. Navy and U.S. USMC senior commanders, respectively—are responsible for the implementation of SECNAV’s policies. CHINFO PA Support and DIRPA (U.S. Navy and USMC, respectively) provide command support for PAO.

<sup>99</sup> Who is also the Deputy CHINFO for Marine Corps Matters.

<sup>100</sup> SECNAVINST 5720.44C, *Department of the Navy Public Affairs Policy and Regulations*, pp. 1-10.

**PAO:** It is the role of the commander to ensure PAOs have the adequate clearance and access to policy and classified information in order to best serve the government's interests. The PAO at each activity is required to review material prepared for public release to ensure it does not reveal classified information or CUI. The PAO is ultimately responsible for releasing information to the public—even if it includes other originators of the data, such as subordinate commands and/or other U.S. Government agencies. If there are other originators, the PAO may coordinate with the CSM who will consult with those commands or agencies to ensure classified information and / or CUI is not released, which could require review with others within the DON or with outside agencies.

**U.S. Navy Personnel Acting in an Official Capacity:** The official duties of many DON personnel require them to provide information and agency records to members of the public, which may include you, the CRM. As such, you should be sensitive to the functions performed by PA personnel and bring matters that may have PA implications to their attention as you learn of them. If your official duties do not include providing information or records to the public, you should refer all requests for information to the appropriate PAO or FOIA authorities.

## **Operational Security**

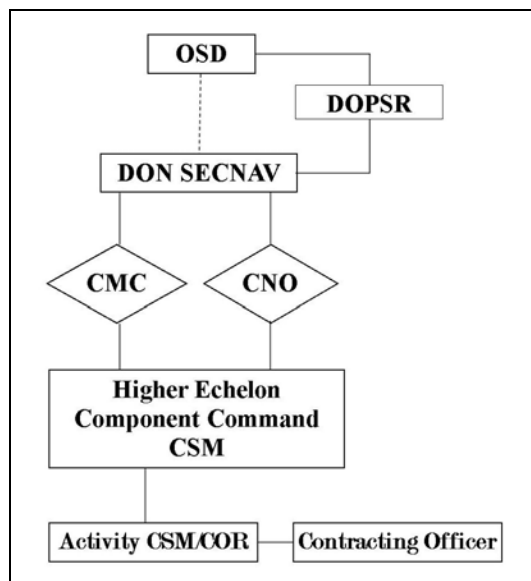
The goal of OPSEC is to deny U.S. adversaries information they do not already have. This may include information that has previously been developed or synthesized, but it often includes observable or detectable activities or information that can be pieced together by someone outside the military to reveal sensitive information regarding a command's operation. Such activities or information can serve as clues about a military activity that adversaries can analyze and exploit to their advantage. OPSEC enables mission success by preventing the inadvertent compromise of such activities, capabilities, or intentions at the tactical, operational and strategic levels. OPSEC is a critical process for all DON activities and these practices must be followed in the daily application of military operations.

**Installation / Activity OPSEC Program Manager:** As with PA, there are OPSEC offices at each echelon. However, since OPSEC information is particular to each echelon and review occurs at that echelon it is less important, as a CRM, for you to know the OPSEC chain of command. The OPSEC Manager at an installation / activity:

Develops, manages and executes the OPSEC program, which focuses on command involvement, planning, assessments, surveys, training, education, threat, resourcing, and awareness. The OPSEC Manager may be full or collateral duty and the responsibilities include: establishing CILs, reviewing contracts to ensure OPSEC responsibilities are properly reflected, and lead OPSEC working group meetings. The OPSEC Manager will also develop a Command OPSEC policy, to include instructions on proper methods to obtain OPSEC reviews of documents proposed for public release, such as CRM reports.

## Information Security Program

The DON ISP establishes 1) uniform policies and procedures for classifying, safeguarding, and declassifying NSI; 2) implements EO 13526, *Classified National Security Information*; 3) implements EO 12829, *The National Industrial Security Program*; and 4) incorporates INFOSEC policies and procedures established by other executive branch agencies. The DON ISP includes



roles and responsibilities for the U.S. Navy and the USMC, and has a direct relationship with DOPSR (Figure 8).

**DOPSR:** The DON interacts with DOPSR for reviews that are under their purview or as needed for additional input. DOPSR is responsible for conducting security and policy review for clearance of official DoD information proposed for official public release by the DoD and its employees (military and civilian). They protect classified information / CUI while making accurate and unclassified information available to the public and Congress to help them understand defense strategy and national security issues.

Figure 8. U.S. Navy, CSM Organization Chart

**DON SECNAV:** SECNAV is responsible for implementing an ISP per the provisions of EOs, public laws, and directives issued by the National Security Council, DOE, DoD, and other agencies regarding the protection of classified information.

**CNO/CMC:** The CNO is responsible to the SECNAV for establishing, directing, and overseeing an effective DON ISP, and for implementing and complying with all directives issued by higher authority. The CMC administers the DON ISP within the USMC and designated functions are performed by specific organizations within the Headquarters, USMC.

**CSM:** The CSM is responsible for coordinating with program managers and procurement officials to ensure that classified information and / or CUI is not released.<sup>101</sup> The CSM is responsible for implementing the ISP and has direct access to the commanding officer. The CSM has many duties with regard to safeguarding information, including coordinating/maintaining SCG, maintaining a liaison with the PAO, coordinating with other commands, developing security measures with regard to visitors who require access to classified information or controlled areas, complying with U.S. Navy requirements with regard to contractors working on

<sup>101</sup> SECNAV M-5510.36, *Personnel Security Program*, pp. 2-6-2-7.



classified contracts, and ensuring that access to classified information is limited to appropriately cleared personnel with a need-to-know.

**Contracting Officer:** For your projects, ultimately it is the responsibility of the Contracting Officer to ensure that no classified information and / or CUI is released. Therefore, as the CRM you might be a COR for the cultural resource technical content, but in addition, the Contracting Officer will also designate in writing one or more qualified security specialists to act as CORs. The specialist(s) will prepare, sign, and revise a DD 254, if required, as well as other security related contract correspondence.

**Security Specialist COR:** The Contracting Officer may designate, in writing, one or more qualified security specialists as CORs who report to the CSM at that echelon. Within larger organizations the likelihood that there will be a specific CSM assigned to the contract as a COR is high, in smaller organizations there may not be an assigned CSM. If a CSM is assigned as COR, that person will prepare and sign the DD 254 and provide revisions thereto. This security COR will also provide other security-related contract correspondence. The COR is responsible to the CSM at their echelon for coordinating with program managers and procurement officials.<sup>102</sup> The security COR will also ensure that industrial security is maintained when classified information is provided to industry for performance on a classified contract.

## **Geospatial-Intelligence**

In general, if you are working with your GIS group at your echelon, they will know whether your project is encroaching upon an NGA issue. However, if you or your contractor adds information to your maps, such as historical missions, building names, uses, training areas, ranges, etc. you may be compiling (aggregating) information that should be protected. The maps you create may be subject to NGA review or oversight. In the DON, if your PAO or CSM has questions about such imagery, it will move to a higher echelon and may be forwarded to NGA for review.

## **Process**

It is DON policy that information will be released as expeditiously as practical and from the lowest possible echelon that is consistent with DON release policies and required reviews. As noted above, for cultural resource projects you will require a CSM and PAO review (with OPSEC component).

As the CRM you will be responsible to oversee the work of your contractor and you may serve as the COR. To support the contractor and the Contracting Officer, you should be familiar with the issues of classified information and conduct some initial project research to determine whether classified information could be an issue on the contract. If classified information was not identified at the outset of the project, as soon as you think there may be an issue, it is

---

<sup>102</sup> Ibid.

important to inform your Contracting Officer, security COR (if one has been assigned), the echelon CSM, OPSEC Manager, and PAO to coordinate items that may affect the contract and to develop a plan for review. The earlier your CSM, OPSEC Manager, and PAO know that you may be forwarding a project, the more likely it is that your deliverable will fit well into their schedule and be reviewed quickly. As noted above, on DON contracts the CSM also acts as a COR for larger organizations, so it is likely that if you are in a larger organization the CSM will be aware of your project throughout the duration. However, if you are in a smaller organization, the CSM will not automatically be included by your Contracting Officer. As such, you should ensure this line of communication is open as your project moves forward.

Certain types of information will require that your deliverable move to a higher echelon or possibly to DON SECNAV or DOPSR. If your project does not include “red flag” data,<sup>103</sup> your review can occur entirely within your activity. However, depending on your project content, your CSM, OPSEC Manager, or PAO may still request review from a higher echelon within the DON or another agency within or outside the DoD. The request for another agency review will occur if your deliverable includes data from that agency and the CSM, OPSEC Manager, or PAO has identified them as the originator of the equity. They may also send the deliverable up the chain of command if there is a question about the sensitivity of the data.

Generally this conversation and transfer of your CRM product will occur from PAO to PAO and from CSM to CSM. OPSEC reviews should be accomplished at the lowest levels to ensure full adherence to OPSEC requirements and restrictions. *OPSEC reviews are generally not sent up the chain of command, as they are based on specific CILs at the local level.* On the PAO side, reviews can move to higher echelons—the highest the product is likely to go is CHINFO. On the CSM side, your deliverable can move to DON SECNAV or DOPSR. The decision of who will review the product will be determined by CMC or CNO. In either case, unless the classified data issues are fairly easy to resolve, these two echelons will likely work together and pass the deliverable back and forth to ensure all issues have been reviewed thoroughly. If they feel the document requires additional SME review, it will be sent back to your headquarters CRM for review. Once that is completed, it will then be passed back to DON SECNAV or DOPSR. Also, as with other levels in the chain of command, it may also be sent out for other agency review. After the review is completed, your document could be sent back to your command with an approval or recommendations from whichever entity originally received the deliverable (Figure 9).

---

<sup>103</sup> See section on Project Process, Phase I for more information on red flag issues.

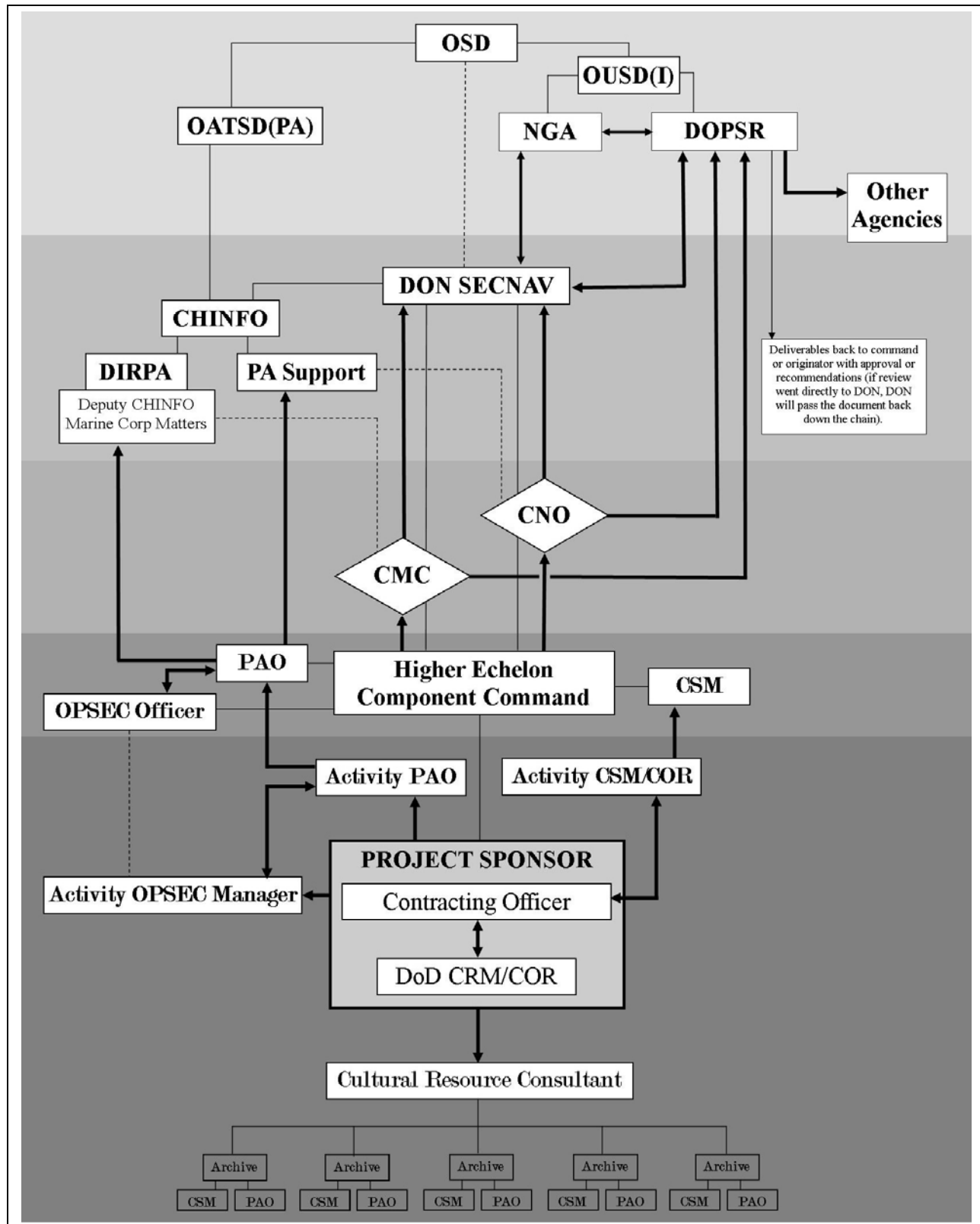


Figure 9. U.S. Navy, Simplified CRM Security and Policy Review Chart

## Basic Review Times

The best way to streamline your review is to communicate early with your PAO, OPSEC Manager, and CSM so they know the basic precepts of your project and generally when your submittal will be coming to them for review. Below are the approximate review times, based on a DOPSR review. You should consult with your CSM, OPSEC Manager and PAO to determine the review times required at your echelon. You may also want to build more time in your schedule if you believe your submittal will be moving up the chain of command to higher echelons or an outside review.

**Presentations/Speeches:** Submit speeches and briefings to DOPSR at least 5 working days before the event at which they are to be presented. Additional time may be needed for complex or potentially controversial speeches due to coordination requirements.

**Papers and Articles:** Submit at least 10 working days before the date that you need the review to be completed. The length, complexity, and content will determine the number of agencies that may be required to review the document and, consequently, the ultimate time required for the complete review process.

**Technical Papers/Reports:** Submit at least 15 working days before the date that you need the review to be completed. This is likely where the bulk of CRM work would fall; again, be sure to work with the local reviewers to understand whether there may be multiple reviews within the DON, whether other DoD agencies may be required to review, and whether it may require review outside the DoD.

**Manuscripts and books:** Submit at least 30 working days before the date that you need the review to be completed. More time may be needed if the material is complex or requires review by other agencies. It is likely that such publications will require DON or DOPSR review.

## Submittals

All information submitted for review should be coordinated within the originating DoD Component to ensure that it reflects the organization's policy position. As noted above, the submittal should be reviewed by PAOs, OPSEC Managers, and CSMs at the lowest echelon and only be sent further up the command chain if it is necessary. Only the full and final text of material proposed for release shall be submitted for review at the DON SECNAV and DOPSR level. These higher echelons will return draft or incomplete documents without action.

However, as noted above, at an earlier point in your project you may want to consult with your local CSM, OPSEC Manager, and / or PAO using notes, outlines, briefing charts, etc. to know whether your project may be headed for a higher review. The addresses below are only to be used if your document could not be cleared internally at the highest DON echelon.

**Paper Submittals:** A minimum of three hard copies and a signed DD Form 1910, *Clearance Request for Public Release of Department of Defense Information*, to the:

Chief, Defense Office of Prepublication and Security Review  
Department of Defense  
Defense Office of Prepublication and Security Review  
1155 Defense Pentagon  
Washington DC 20301-1155

OR

DUSN PPOI  
ATTN: DUSN SECURITY  
1000 Navy Pentagon, Room 4E572  
Washington, DC 20350-1000

**Electronic Submittals:** These are not recommended unless you are using secure means of transmittal, otherwise you have the potential of “electronic spillage” and your computer may need to be “scrubbed.” If you do have a secure email, you can submit one copy in Microsoft Word with a signed DD Form 1910, by e-mail to:

[whs.pentagon.esd.mbx.secrev@mail.mil](mailto:whs.pentagon.esd.mbx.secrev@mail.mil) (Unclassified information only)

OR

[Don\\_security\\_info\\_pers\\_us@navy.mil](mailto:Don_security_info_pers_us@navy.mil)

**Abstracts, Papers, and Presentations:** Abstracts that are to be published in advance of a completed document require clearance. Such clearance does not fulfill the requirement to submit the full text for review prior to its presentation or publication. If an abstract has been cleared in advance, the previous clearance and attached case number needs to be noted on the DD Form 1910 or other transmittal when the full text is submitted.

**Websites:** Information intended for placement on websites, or other publicly accessible computer servers, which are available to anyone, without access controls, may require review and clearance for public release. Your website clearance questions should be directed to your component’s website manager.

## Possible Outcomes

**Cleared:** Information may be released to the public without restriction.

**Cleared as Amended:** Amendments are mandatory due to deletions or additions—DoD clearance is contingent upon the implementation of the noted amendments. The information may be released without restriction upon implementation of the amendments.

**Recommended Changes:** These are non-binding suggested changes to clarify or amplify information in the document.

**Not Cleared:** The information is not cleared and may not be publicly released.

**Returned Without Action:** This occurs when the reviewer is unable to review due to insufficient time, the material is already in the public domain, or the review may be cancelled upon request of submitter.

# DEPARTMENT OF THE AIR FORCE DOCUMENT REVIEW PRACTICES

## **Purpose**

The Air Force has an ongoing effort to inform and increase public understanding of their mission, operations, and programs. While sharing information in a timely manner is their goal, it is important to ensure that CI and CUI be reviewed prior to public release so the U.S. does not release classified or otherwise protected information. The Air Force Public Affair, Security and Policy Review (SP&R) objective is to ensure “maximum clearance of information in minimum time.”<sup>104</sup>

The Air Force process includes two aspects of information management: OPSEC and SP&R. In an effort to ensure non-releasable information is not disclosed to the public, all articles, papers, presentations, and other material must go through these reviews, to ensure that information released in the public domain is accurate, does not include classified material, supports OPSEC requirements, and is consistent with established policies of the Air Force, DoD, and Federal Government.

## **Roles & Responsibilities**

As the CRM, it is your responsibility to ensure that your projects are submitted to the OPSEC Program and SP&R office before disseminating in the public domain. The SP&R office will ensure SME review of the document prior to security and policy review clearance.

## **Operational Security Program**

Air Force organizations must develop and integrate OPSEC into their mission planning to ensure CI and indicators are identified. At a minimum, the Air Force will integrate OPSEC into the following missions: military strategy, operational and tactical planning and execution, military indoctrination, support activities, contingency, combat and peacetime operations and exercises, communications-computer architectures and processing, critical infrastructure protection, weapons systems, RDT&E, Air Force specialized training, inspections, acquisition and procurement, medical operations, and professional military education. Although the OPSEC program helps commanders make and implement decisions, the ultimate decisions are the commander’s responsibility. Commanders must understand the risk to the mission and then determine which countermeasures are required.

---

<sup>104</sup> Secretary of the Air Force. AFI 35-102, *Public Affairs: Security and Policy Review Process*, 20 October 2009, p. 2 and 7.

**The Deputy Chief of Staff for Operations, Plans and Requirements:** This is the office of primary responsibility (OPR) for implementing DoD OPSEC policy and guidance. It has assigned responsibility to Director of Cyber and Space Operations, which established the Air Force OPSEC program including assessments, surveys, training, education, threat analyses, resourcing, and awareness.

**Higher Headquarters, OPSEC Program Manager:** Major Commands, Field Operating Agencies, and Direct Reporting Units implement AF OPSEC guidance that incorporates and institutionalizes OPSEC concepts into relevant doctrine, policies, strategies, programs, budgets, training, exercising, and evaluation methods. This position is within the operations or plans element and serves as the POC for all OPSEC related issues between headquarters Air Force and the command.

**Wing / Installation Commanders and Directors:** Issue guidance regarding OPSEC measures to all assigned personnel to ensure OPSEC is integrated into day-to-day and contingency operations. They retain responsibility for risk management decisions and the overall implementation of countermeasures, and must determine the balance between countermeasures and operational needs. Wing / installation commanders and directors appoint a primary and secondary OPSEC Program Manager.

**Primary / Secondary OPSEC Program Managers:** OPSEC Program Managers advise the commander / director on all OPSEC and related matters, including the development of operating instructions, guidance, and OPSEC measures. They incorporate OPSEC into organizational plans, exercises, and activities; develop, implement, and distribute commander's OPSEC guidance memorandums; and ensure procedures are in place to control CI and associated indicators. They work closely with PA, information protection, website administrators, and other officials designated by the commander who share responsibility for the protection and release of information to ensure CI is protected.<sup>105</sup>

### **Public Affairs and Information Security Program**

The Air Force is obligated to provide the public with maximum information about Air Force operations and activities, without compromising protected information. The SP&R program works to clear, without delay, the maximum amount of information at the lowest competent review level. Information that requires a SP&R review is that which relates to the plans, policies, programs, or operations of DoD or the U.S. Government. Whether information is prepared as an official release or a personal enterprise, it must be reviewed and cleared before it is released. SP&R is responsible for carrying out security and policy reviews.

---

<sup>105</sup> Other offices and activities have roles and responsibilities in the AF OPSEC process. Refer to AFI 10-701, *Air Force Operations Security (OPSEC)*, 8 June 2011 for the full list and more information.



**The Secretary of the Air Force, Office of Public Affairs (SAF/PA)** develops policy and guidance to ensure a security and policy review has been completed and that OPSEC has been considered prior to releasing information to the public.

**Major Commands, Field Operating Agencies, Direct Reporting Units, and installation-level organizations:** Each echelon has a PA organization. Clearance authority is delegated to the PA organization at the lowest echelon qualified to evaluate the contents and implications of the subject. Information whose review originates at the installation level will be moved to higher echelons, if necessary.

### **Geospatial-Intelligence**

In general, if you are working with your GIS group at your echelon, they will know whether your project is encroaching upon an NGA issue. However, if you or your contractor adds information to your maps, such as historical missions, building names, uses, training areas, ranges, etc. you may be compiling (aggregating) information that should be protected. The maps you create may be subject to NGA review or oversight. In the Air Force, if PA has questions about such imagery, your project will move to a higher echelon and may be forwarded to NGA for review.

### **Process**

#### **Operational Security Program**

Prior to submitting documents to PA for a security and policy review, you must coordinate your request first through an OPSEC review. You should meet with the OPSEC Program Manager at your echelon during the project planning and implementation phase. At the wing / installation level, OPSEC Program Managers reside in the operations or plans element. If you are a member of a tenant organization on a larger installation / activity, you should seek out your tenant organization OPSEC Program Manager.

The OPSEC Program Manager is responsible for reviewing all information intended for publication or release to the public.<sup>106</sup> The OPSEC Program Manager and PA at your echelon work closely together to ensure there are no unauthorized disclosures. It is likely that they have developed guidance specific to their echelon on how to protect CI. Such guidance will include turn-around times, submittal formatting information, and possible outcomes of the review. If you cannot obtain this written guidance, or if you are unclear of the requirements, you should ask the OPSEC Program Manager for more information *before* you submit documents for review. Once your information is cleared through the OPSEC review, you are then ready to submit your product to PA.

---

<sup>106</sup> This review could include, but is not limited to, base newspapers, safety magazines, flyers, web pages, interviews, and information for news articles.

## Public Affairs and Information Security

A security and policy review will identify the presence of classified information or CUI; it will not result in the classification or declassification of material. In addition, once SP&R has reviewed your product,<sup>107</sup> you may receive a clearance. This is notification that the product does not require safeguarding; however it is not the approval for the release of information. The actual release of the information resides with you, as the originator, who must work in coordination with your chain of command to actually provide the information to the public. If SP&R determined that your product could not be released, the OPR for the military material or mission described will determine the security classification of the material based on the applicable Security Classification Guide.<sup>108</sup>

For Example: You have developed a Section 110 report detailing the significance of a Minuteman missile site at your Air Force Base. The installation (or its Major Command), as the originator, would ultimately decide if the report would be released to the public. If you had developed a report that could not be released to the public, the associated OPRs could include: DoD / DOE, for information on the nuclear warhead on Minuteman; Air Force (specifically, the 526th ICBM Systems Group), for information on the accuracy of the missile or the blast hardness of the silo.

Although AFI 35-102 provides specific review periods, there are always extenuating circumstances that may dictate a longer review process with additional SMEs. It is important to identify military topics that may trigger longer reviews for your project. A DOPSR and SAF/PA A-level Clearance is required for many topics, but those that are most likely to be triggered during a cultural resource project are a product that:

1. Contains technical data, including data developed under contract or independently developed and controlled by the ITAR that may be militarily critical and subject to limited distribution, but on which a distribution determination has not been made.
2. Military activities or applications in space, nuclear weapons, including weapon-effects research; chemical and biological warfare issues; biological and toxin research; high-energy lasers and particle beam technology; arms control treaty implementation.<sup>109</sup>

Because the process can include multiple echelons and reviews from other agencies: *It is important that you do not make date-of-delivery commitments to entities outside the Air Force until your product has been cleared for public release.*

---

<sup>107</sup> This could include a paper or presentation, abstracts about a paper, article for a magazine or other publication, and deliverables from consultants.

<sup>108</sup> The OPR can be identified through the authorship of existing SCGs that relate to the topics in your products.

<sup>109</sup> AFI 35-102, *Public Affairs: Security and Policy Review Process*, p. 3.

If, at the outset of a project, you know that classified data is part of the project, the following should be included in the contract with your consultant:

- DD Form 254, *Department of Defense Contract Security Classification Specification*
- DoD 5220.22-R, *Industrial Security Regulation*
- DoD 5220.22-M, *National Industrial Security Program Operating Manual*

Once the deliverables are ready for review, the contractor is required to submit the material that is proposed for public release according to the requirements specified in the above documents.

It is important to remember that although you may not have anticipated a classified project—and therefore did not include the contract requirements noted above—CUI can easily be identified as something that should be classified when it has been rewritten / combined with other information. This type of information is referred to as “aggregate information.” This is of great concern when working with cultural resource documentation, as the job of historians is to “put the information back together again.”

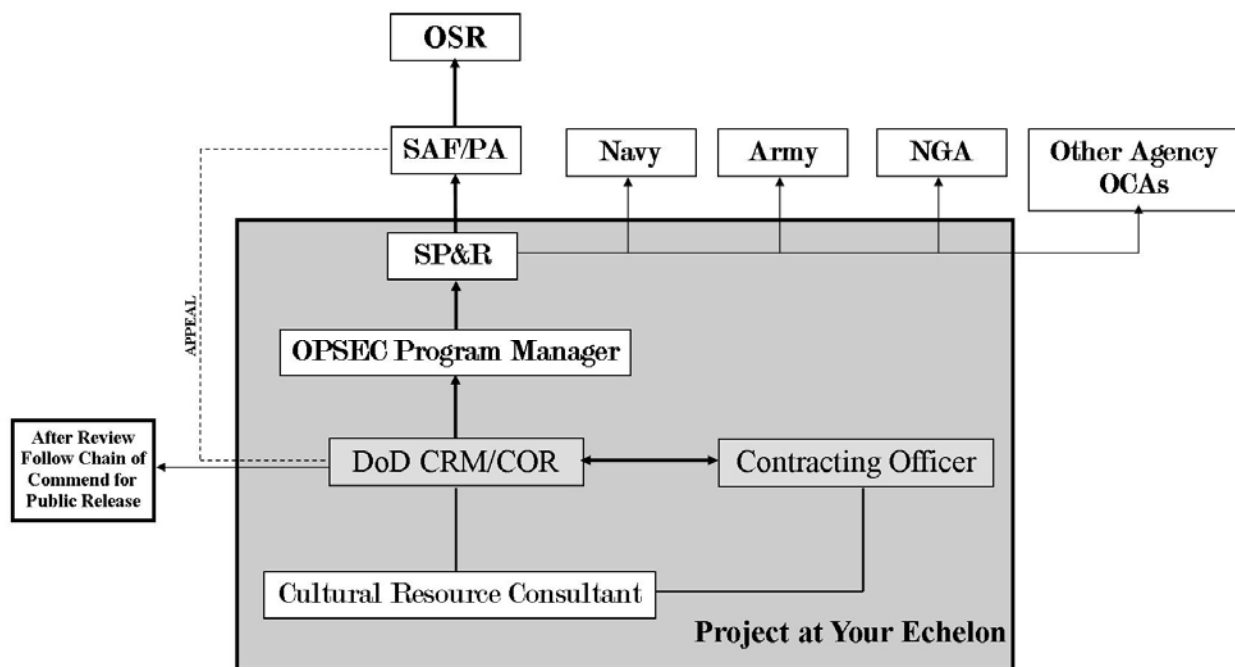


Figure 10. U.S. Air Force, Simplified CRM Security and Policy Review Chart

### Basic Review Times

- For planning purposes allow at least 10 work days for each Air Force level of review.
- For other DoD or Federal agency review, allow 20 work days.

While AFI 35-102 denotes these review times, it is important to keep in mind that the review period depends on how many cases are in the queue for a security and policy review and the

volume/complexity of the product you are having reviewed. If the item includes data from other services, it will require a review from each DoD Component. And, as noted earlier, if your case requires additional reviews above the originating echelon, it will require additional time to conduct the reviews.

### **Submittals**

Documents being submitted for a security and policy review can be submitted via email if the classified SIPRNet computer system is used. It should not be submitted via the unclassified NIPRNet system or through other unclassified digital means as FOUO is often revealed during the security and policy review process—since you won’t know up front whether there is FOUO, transfer should take place through secured means.

Work with the PA staff in your echelon to determine the current minimum requirements for all submissions and how many copies they require. As an example: if your submission moves up the chain of command to the SAF/PA, according to AFI 35-102, the SAF/PA will require 6 paper copies for an Air Force-level review. If the submission requires a DoD clearance, the SAF/PA will require an additional 6 paper copies with the initial submission.<sup>110</sup> After the Air Force review and revisions by the originator—when the document is ready for a DoD review—the submission requires an additional 4 paper copies.<sup>111</sup>

When you are submitting technical materials, which most cultural resource reports are, include an abstract (either as part of the report or in the transmittal) in layman’s terms and text about why it is important for the DoD to release the information.

When submitting a product for review you should include a memo with the following:

- Name, title, and originating unit, author or speaker
- Title of the product
- Statement on where, when, and how the information is to be released and the sponsoring organization
- Clearance date you require and provide a reason (needs to be complete by x in order to make publication deadline or be available to installation commander for his use, etc.).
- Statement that information has been reviewed at appropriate echelon and is recommended for public release (if it is at your level, state you have reviewed it; if it has been reviewed by SP&R and they have recommended a higher review, state that).
- Signed or initialed notation by author or speaker indicating approval of the text.
- If review is moving to Air Force-level, be sure the SP&R staff have provided a statement “on technical material that export restrictions and militarily critical technologies as well

---

<sup>110</sup> The AFI is not clear on how many copies a video or other non-paper submittal would require.

<sup>111</sup> AFI 35-102, *Public Affairs: Security and Policy Review Process*, p. 5.

as current Air Force and DoD policies have been considered. Provide all relevant comments from field unit technical coordinators and attach contractor transmittal letter, if it contains pertinent data.”<sup>112</sup>

You will need to submit the required information and correct number of copies through the appropriate channels to the local SP&R office for a security and policy review. Once SP&R receives your product and the memo, they will:

1. Log in your submittal as a case;
  2. Review the material to determine which agencies and staff must review;
  3. Establish a suspense date; and
  4. Dispatch the case for review.
- If your product is audiovisual, the video AND script will be reviewed to determine whether a coordinated viewing with other agencies and staff needs to be arranged.
  - After the review has been completed by agencies and staff, the reviewer will evaluate comments and contact agencies to resolve issues. Once that is complete, the reviewer will determine the releasability (also known as a clearance position) of the material.
  - After the reviewer determines a clearance position, the review action is either completed or the case is sent to the next review echelon, which repeats the process.
  - Once cases have been returned from higher-echelon review, the SP&R will retain one file copy showing the final clearance with changes and markings to the material, plus copies of each reviewing organization’s signed remarks.
  - A copy of the material officially cleared by letter or stamp, with final review markings and annotated changes, or, alternatively, correspondence explaining a denial of clearance will be sent to you, the originator.
  - After the security and policy review has been completed, the reviewer will evaluate comments and contact agencies to resolve issues (if applicable) and provide the originator with a copy of the cleared document and any recommendations/amendments (if applicable). The final review of the document will be affixed with a “cleared for public release stamp”, with final review markings and annotated changes, or, alternatively, correspondence explaining a denial of clearance will be sent to you, the originator.

---

<sup>112</sup> Ibid.

## Possible Outcomes

Below is a list of the possible outcomes of an Air Force security and policy review.

**Cleared for Public Release:** The document is cleared as submitted—no changes required.

**Cleared with Recommendations:** This is not the responsibility of a security and policy review; however, the reviewer can make edits for clarity and accuracy. Editorial reviews are marked with a line through the text and written edits, rather than brackets which denote non-releasable information.

**Cleared as Amended:** The security and policy review may result in markups that identify text for mandatory removal prior to publication. The text for removal will be bracketed and may include substitute language written above that which is bracketed for removal.

**Objection:** There can be an overall objection to clearing your case. If this happens, the reviewer does not have to mark up the document, but will provide you with a detailed justification. This can occur when a case requires extensive amendment or rewrites.

NOTE: If a document receives an objection, the originator can appeal the decision that has been made by the security and policy review through a formal written appeal to SAF/PA. Such an appeal must include “strong supporting rationale and authoritative evidence.”<sup>113</sup> If SAF/PA cannot resolve the appeal, it may be sent to a higher echelon within the Air Force or to DOPSR.

---

<sup>113</sup> AFI 35-102, *Public Affairs: Security and Policy Review Process*, p. 9.

## RESOURCES

### **Defense Office of Prepublication and Security Review**

DOPSR Help Desk Staff:

Tel: 703-614-5001

FAX: 703-614-4956 (U)

Email: [whs.pentagon.esd.mbx.secrev@mail.mil](mailto:whs.pentagon.esd.mbx.secrev@mail.mil) (Unclassified information only)

DOPSR website: <http://www.dtic.mil/whs/esd/>

The DOPSR website has several helpful documents concerning the Security and Policy review process, including “How to Submit an SR Request,” “DOPSR SR Brochure,” “SR Information Sheet,” and “SR Guidelines.”

### **Department of the Army**

HQDA, Army G-2 Information Security is the office responsible for providing policy, practices and procedures for the Army INFOSEC Program as it relates to the protection of classified NSI and CUI. More information concerning the Army program is available at:

<http://www.dami.army.pentagon.mil/site/InfoSec/>.

The Information Security Team Lead at 703-695-2644 should be contacted for questions concerning the Army INFOSEC program, including classification, declassification, and security and policy reviews.

### **Department of the Navy**

The Deputy Under Secretary of the Navy, Plans, Policy, Oversight and Integrations is the Security Executive for the DON (to include USMC). Comprehensive information concerning the DON security program is available at: <http://www.secnav.navy.mil/ppoi/security>. This address can also be used for other questions concerning:

- Declassification program
- Classification guides
- OCAs
- Security reviews
  - Mandatory declassification reviews
  - Prepublication reviews
  - Congressional reviews

### **Department of the Air Force**

The Secretary of the Air Force / Security Office has primary responsibility for the Air Force INFOSEC program.

SAF/PA has primary responsibility for the AF Security and Policy review process.

SAF/PA  
1690 AF Pentagon  
Washington, DC 20330-1690  
703-697-6061

### **Defense Security Service**

The Defense Security Service Center for Development of Security Excellence provides access to security training, education, and certification for DoD and industry. Of particular interest to CRMs should be the basic, online, introductory courses in General Security and INFOSEC. Visit their website at <http://www.cdse.edu/index.html> for more information.

### **Defense Technical Information Center**

The Administrator, DTIC, under the authority, direction, and control of the Under Secretary of Defense for Acquisition, Technology, and Logistics maintains an index of SCGs in an online database accessible through [www.dtic.mil](http://www.dtic.mil). This is a restricted website and requires a DTIC account to access.

### **Security Classification Guides**

DTIC maintains the “Security Classification Guide–Formerly Security Classification Guide Index” as part of its DoD Techipedia website at <https://www.dodtechipedia.mil/dodwiki/x/t4QqB>. The online index includes lists of current and historical (cancelled or superseded) SCGs, as well as SCGs by DoD Component, DoD Activities, and Joint DoD / DOE SCGs. Many of the current 1,780 SCGs are available through this site; however, historical SCGs are not located at DTIC.<sup>114</sup>

### **DoD Scientific and Technical Information Program**

DoD established STIP to “improve and enhance the acquisition of data sources, prevent redundant research, disseminate technical information efficiently, prevent the loss of technical information to U.S. adversaries and competitors, and aid the transfer of technical information to qualified researchers in U.S. industry and government agencies.”<sup>115</sup> As part of its STIP training initiative, DTIC provides several resources useful to the research and production of CRM documents, including a current list of all relevant policy, guidance and reports, as part of the training portion of its website at:<http://www.dtic.mil/dtic/customer/training/stinfo/stinfodocs.html>.

---

<sup>114</sup> Hyperlinks to PDFs of the SCGs are included in the Index.

<sup>115</sup> <http://www.dtic.mil/dtic/customer/training/stinfo/>



### **DTIC Customer Support**

DTIC maintains a reference team to assist researchers with DTIC programs and resources. Their support website at <http://www.dtic.mil/dtic/customer> has current points of contact to help you find DTIC reports and information; the site also has an online “Ask a Librarian” function.

Intentionally Blank

## DEFINITIONS

**Aggregation**

A collection of preexisting unclassified items combined to result in information that should be protected (also known as compilation).

**Authorized Holder**

Anyone who satisfies the conditions for access to classified information as stated in Section 4.1 of EO 13526.

**Automatic Declassification**

The declassification of information based upon the occurrence of a specific date or event as determined by the OCA or the expiration of a maximum time frame for duration of classification defined under EO 13526.

**Case (Air Force)**

A deliverable that has been logged in for a Security and Policy Review. In the Air Force, if the reviewing organization has more than 50 cases annually, the case will be logged into the Public Affairs Release System (PAIRS).

**Classification**

Classification is the determination by an authorized official that official information requires—in the interests of national security—a specific degree of protection against unauthorized disclosure.

**Classified Information**

Information that has been determined to require protection against unauthorized disclosure in the interest of national security; it is classified for such purpose by an appropriate classifying authority per the provisions of EO 13526.

**Controlled Unclassified Information [CUI]**

Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

**Collateral Information**

Information identified as NSI under the provisions of EO 13526, but which is not subject to enhanced security protection required for SAP or other compartmented information. It generally refers to Top Secret, Secret, or Confidential information.

**Compartmented**

Certain types of classified information that relate to specific national-security topics or programs whose existence may not be publicly acknowledged, or the sensitive nature of which requires special handling. Usually associated with SCI or SAP.

**Compilation**

A collection of preexisting unclassified items combined to result in information that should be protected (also known as aggregation).

**Confidential**

A classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the OCA is able to identify or describe.

**Critical Nuclear Weapons Design Information [CNWDI]**

Top Secret or Secret RD that reveals the theory of operation or design of the components of a thermonuclear or implosion type fission bomb, warhead, demolition munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable and high explosive material by type. Among these excluded items are the components that personnel set, maintain, operate, test, or replace.

**Critical Program Information**

Elements or components of a Research, Development and Acquisition program that, if compromised, could cause a significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction or; enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. Examples of critical program information for a Research, Development and Acquisition program may include: components, engineering design, manufacturing processes, critical technologies, system capabilities and vulnerabilities, and other information that give the system its distinctive operational capability.

**Critical Technology**

Technology that consists of: arrays of design and manufacturing know-how (including technical data); keystone manufacturing, inspection, and test equipment; keystone materials; and goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the U.S. (also referred to as militarily critical technology).

**Declassification**

The authorized change in the status of information from classified information to unclassified information.

**Derivative Classification**

The incorporating, paraphrasing, restating, or generating, in new form, information that is already classified and ensuring that it continues to be classified by marking or similar means when included in newly created material.

**DoD Component**

The Office of the Secretary of Defense, the Military Departments (Air Force, Army, Navy), the Chairman of the JCS, the Combatant Commands, and the Defense agencies.

**DoD Unclassified Controlled Nuclear Information (UCNI)**

DoD unclassified information on security measures (including security plans, procedures, and equipment) for the physical protection of DoD SNM, equipment, or facilities.

**Downgrading**

The determination by an approved authority that information classified at a specific level requires a lower degree of protection, therefore, reducing the classification to a lower level.

**Duration of Classification**

A specific date or event, as established by the OCA, for automatic declassification of information based upon the duration of the national security sensitivity of that information as established by EO 13526.

**Foreign Government Information [FGI]**

FGI is information received from one or more foreign governments or international organizations as classified or expected to be held in confidence. It is classified, safeguarded, and declassified as agreed between the U.S. and the foreign entity.

**Formerly Restricted Data [FRD]**

Information removed from the DOE RD category upon a joint determination by the DOE (or antecedent agencies) and the DoD that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as RD.

**For Official Use Only [FOUO]**

A marking applied to unclassified information that meets one or more exemptions of FOIA under U.S.C. Title 5, Section 522 (b) (2) through (9). Information must be unclassified to be designated FOUO. Declassified information may be designated FOUO, if it qualifies under exemptions (2) through (9).

**For Official Use Only Law Enforcement Sensitive [FOUO-LES]**

A marking applied to unclassified information that meets one or more exemptions of FOIA under U.S.C. Title 5, Section 522 (b)(2) through (9). It is intended to denote that the information was compiled for law enforcement purposes.

**Freedom of Information Act [FOIA]**

A law that established the public right to inspect, review, and receive copies of government records. This applies to all records except for those exempt from release under the Act, which are generally: Classified Records, Internal Personnel Rules and Procedures, Records exempt from release by other Statutes, Records containing Confidential Commercial Information,

Records otherwise privileged in Civil Litigation, Invasion of Personal Privacy (Privacy Act) (e.g., home addresses), Records related to open investigations.

**Information**

Any official knowledge that can be communicated or documentary material—regardless of its physical form or characteristics—which is owned by, produced by or for, or is under the control of the U.S. Government. “Control” means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

**Mandatory Declassification Review**

Review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.5 of EO 13526.

**Marking**

The physical act by a reviewer to indicate on classified material: the assigned classification, changes in classification, downgrading and declassification instructions, and any limitations on the use of the classified information.

**National Security**

National defense or foreign relations of the U.S.

**National Industrial Security Program [NISP]**

National program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the U.S. Government and serves as a single, integrated, cohesive industrial security program to protect classified information and preserve U.S. economic and technological interests.

**National Security Information [NSI]**

Any official information that has been determined under EO 13526, or any predecessor order, to require protection against unauthorized disclosure and is so designated. This includes non-military information that should be classified in the “interest of national security.” The designations Top Secret, Secret, and Confidential are used to identify such information which is commonly referred to as “classified information.”

**Need-to-know**

A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized U.S. Governmental function.

**Non-Collateral**

Information that is classified Secret or Top Secret also falls under an SCI or SAP designation is considered non-collateral.

**Not Releasable to Foreign Nationals [NOFORN]**

An intelligence control marking used to identify information which an originator has determined may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval.

**Original Classification**

An initial determination made by the OCA that information requires, in the interest of national security, protection against unauthorized disclosure.

**Original Classification Authority [OCA]**

An official authorized in writing, either by the President, an agency head, or other official designated by the President “to classify information originally” or “to make an original classification decision.” If you are not an OCA, but believe information should be classified, you are allowed to provide a Tentative Classification.

**Records having permanent historical value**

Presidential papers or Presidential records and the records of an agency that NARA has determined should be maintained permanently in accordance with title 44, United States Code.

**Restricted Data (RD)**

All data concerning: the design, manufacture, or utilization of atomic weapons; the production of SNM; or the use of SNM in the production of energy, but shall not include data declassified or removed from the RD category under Section 142 of the Atomic Energy Act, as amended.

**Safeguarding**

Measures and controls prescribed to protect classified information.

**Secret**

A classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security, that the OCA is able to identify or describe (E.O. 12598, as Amended).

**Security Classification Guide [SCG]**

The primary reference source for derivative classifiers to identify the level and duration of classification for specific informational elements. OCAs are required to prepare an SCG for each system, plan, program or project under their cognizance that creates classified information.

**Sensitive But Unclassified [SBU]**

Information that is originated within the DOS and warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the FOIA. (Previously "Limited Official Use" (LOU) in the DOS).

**Sensitive Compartmented Information [SCI]**

Classified information concerning or derived from intelligence sources or methods, or analytical processes that is required to be handled within formal access control systems established by the DCI.

**Special Access Programs [SAPs]**

A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

**Systematic Declassification Review**

The review for declassification of classified information contained in records that have been determined by the Archivist of the U.S. to have permanent historical value per Chapter 33 of Title 44, U.S.C.

**Technical Data**

Recorded information related to experimental or engineering works that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul material. The data may be graphic or pictorial delineations in media such as drawings or photographs, text in specifications or related performance or design type documents, or computer printouts. Examples of technical data include research and engineering data or drawings, associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications, and related information and computer software documentation.

**Technical documents**

Documents containing technical data or information.

**Technical Information**

Information, including scientific information, which relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment.

**Tentative Classification**

Allows those individuals without OCA, who create information they believe to be classified or which they have significant doubt about the appropriate classification, to mark the information accordingly.

**Top Secret**

A classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security, that the OCA is able to identify or describe (E.O. 12598, as Amended).

**Unauthorized Disclosure**

A communication or physical transfer of classified information to an unauthorized recipient.

**Unclassified Controlled Nuclear Information (UCNI)**

DOE unclassified information on security measures (including security plans, procedures, and equipment) for the physical protection of SNM, equipment, or facilities.



# ANNOTATED BIBLIOGRAPHY

## Office of the Secretary of Defense

These and other DoD policy issuances can be found at <http://www.dtic.mil/whs/directives/>.

## Industrial Security

- Under Secretary of Defense for Intelligence. DoD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program*, 2 January 1992 (Administrative Reissuance 20 April 1999).  
PURPOSE: Prescribe the policy, responsibilities, and procedures for the clearance program for Federal employees and contractors. This is the Directive that carries out the requirements of EO 10865, as amended and it includes the Adjudicative Guidelines for determining eligibility for clearance to access classified information.
- Under Secretary of Defense for Intelligence. DoD Instruction 5220.22, *National Industrial Security Program (NISP)*, 18 March 2011.  
PURPOSE: Establish policy and assign responsibilities for administration of the NISP in accordance with Federal policy and orders to ensure that classified information disclosed to industry is properly safeguarded.
- Under Secretary of Defense for Intelligence. DoD Manual 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, 28 February, 2006, Incorporating Change 1, 28 March 2013.  
PURPOSE: Prescribe the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information; control the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors; prescribe the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including RD, FRD, intelligence sources and methods information, SCI, and SAP information.
- Defense Investigative Service. DoD Regulation 5220.22-R, *Industrial Security Regulation*, 4 December 1985.  
PURPOSE: Prescribe uniform procedures that ensure the safeguarding and protection of classified information made available to industry.

## Geospatial-Intelligence

- Director of Administration and Management. DoD Directive 5105.60, *National Geospatial Intelligence Agency*, 29 July 2009.  
PURPOSE: Define GEOINT; related roles and responsibilities, the relationship of NGA, JCS, DIA, DoD Components, and others; development of standards; the release of information; training; program management; engaging foreign entities; and the associated authorities and administration.

- Under Secretary of Defense for Intelligence. DoD Instruction 5030.59, *National Geospatial Intelligence Agency, LIMITED DISTRIBUTION Geospatial Intelligence*, 7 December 2006.  
PURPOSE: Define the handling of unclassified GEOINT including the roles and responsibilities, and the requirements for heads of DoD Components.
- Under Secretary of Defense for Intelligence. DoD Instruction 3115.15, *Geospatial Intelligence*, 6 December 2011.  
PURPOSE: Define GEOINT operations within the DoD and identify the responsibilities of all the agencies that work with GEOINT.
- Chairman, Joint Chiefs of Staff. JCS Instruction, *Requirements for Geospatial Information and Services*, 10 April 2010.  
PURPOSE: Establish guidance for the identification, prioritization, and submission of GI&S requirements for the Joint Staff, the Services, combatant commands, Defense agencies, and other organizations participating in NSG.

## **Information Security**

- Department of Defense, Special Access Program Central Office. DoD Directive 5205.07, *Special Access Programs (SAP) Policy*, 1 July 2010.  
PURPOSE: Update policy and responsibilities for the oversight and management of all DoD SAPs, and authorize the publication of other SAP issuances, as appropriate.
- Department of Defense, Special Access Program Central Office. DoD Instruction 5205.11, *Management, Administration, and Oversight of DoD Special Access Programs (SAPs)*, 6 February 2013.  
PURPOSE: Establish and implement SAP policy, assign responsibilities, and update and prescribe procedures for the management, administration, and oversight of all DoD SAPs.  
NOTE: This Instruction replaces / reissues DoD Instruction O-5205.11, which is currently referred to in several other DoD INFOSEC policies.
- Under Secretary of Defense for Intelligence. DoD Instruction 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information*, 9 October 2008, Incorporating Change 1, 13 June 2011.  
PURPOSE: Update policy and responsibilities for collateral, SAP, and SCI, and CUI within an overarching DoD INFOSEC Program under applicable Federal and DoD regulations and policies.
- Under Secretary of Defense for Intelligence. DoD Manual 5200.01 (Four volumes), *DoD Information Security Program*, 24 February 2012.  
PURPOSE: This Manual is composed of four volumes, each containing its own purpose. The purpose of the overall Manual is to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of CUI and classified information, including information categorized as collateral, SCI, and SAP.

- *Volume 1: Overview, Classification, and Declassification*, 24 February 2012.  
PURPOSE: Describe the DoD INFOSEC Program and provide guidance for classification and declassification of DoD information that requires protection in the interest of the national security.
- *Volume 2: Marking of Classified Information*, 24 February 2012, Incorporating Change 2, 19 March 2013.  
PURPOSE: Provide guidance for the correct marking of classified information.
- *Volume 3: Protection of Classified Information*, 24 February 2012, Incorporating Change 2, 19 March 2013.  
PURPOSE: Provide guidance for safeguarding, storage, destruction, transmission, and transportation of classified information. Identify security education and training requirements and processes for handling of security violations and compromise of classified information. Address information technology issues of which the security manager must be aware.
- *Volume 4: Controlled Unclassified Information*, 24 February 2012.  
PURPOSE: Provide guidance for the identification and protection of CUI.
- Under Secretary of Defense for Intelligence. DoD Manual 5200.45, *Instructions for Developing Security Classification Guides*, 2 April 2013.  
PURPOSE: Assist in the development of the security classification guidance required for each system, plan, program, or project in which classified information is involved.
- Under Secretary of Defense for Intelligence. DoD Instruction 5210.02, *Access to and Dissemination of Restricted Data (RD) and Formerly Restricted Data (FRD)*, 3 June 2011.  
PURPOSE: Establish policies, assign responsibilities, and prescribe procedures governing access to, and dissemination of data classified as RD and FRD by DoD.
- Under Secretary of Defense for Intelligence. DoD Instruction 5210.83, *DoD Unclassified Controlled Nuclear Information (UCNI)*, 12 July 2012.  
PURPOSE: Update policies, assign responsibilities and prescribe procedures for controlling unclassified information on the physical protection of DoD SNM, equipment, and facilities. Such information is referred to as DoD UCNI, to distinguish it from a similar DOE program.
- Department of Defense. DD Form 254, *DoD Contract Security Classification Specialization*, December 1999.  
PURPOSE: Require that a DD Form 254 be incorporated in each classified contract. The form provides to the contractor / subcontractor the security requirements and the classification guidance that would be necessary to perform on a classified contract. Copy of current form provided in Appendix B of this handbook.

## Operations Security

- Under Secretary of Defense for Intelligence. DoD Directive 5205.05E, *DoD Operations Security (OPSEC) Program*, 20 June 2012.  
PURPOSE: Mandate that OPSEC be considered across the entire spectrum of DoD missions, functions, programs, and activities. The level of OPSEC to apply is dependent on the threat, vulnerability, and risk to the assigned mission, function, program, or activity, and available resources. OPSEC and other security and information operations programs shall be closely coordinated to account for force protection and the security of information and activities.
- Under Secretary of Defense for Intelligence. DoD Manual 5205.02, *DoD OPSEC Program Manual*, 3 November 2008.  
PURPOSE: Provide baseline requirements for DoD Component OPSEC programs to ensure national security-related missions and functions are protected.

## Public Affairs, Security and Policy Review Process, and Public Information

- Under Secretary of Defense for Intelligence. DoD Directive 5210.50, *Unauthorized Disclosure of Classified Information to the Public*, 22 July 2005.  
PURPOSE: Update policy and assign responsibilities for reporting and investigating known or suspected incidents of unauthorized public disclosure of classified information and reporting corrective and disciplinary action taken.
- Under Secretary of Defense for Acquisition, Technology and Logistics. DoD Directive 5230.24, *Distribution Statements on Technical Documents*, 18 March 1987.  
PURPOSE: Update policies and procedures for marking technical documents, including production, engineering, and logistics information, to denote the extent to which they are available for distribution, release, and dissemination without additional approvals or authorizations.
- Director of Administration and Management. DoD Directive 5230.09, *Clearance of DoD Information for Public Release*, 22 August 2008.  
PURPOSE: Update policy and responsibilities for the security and policy review process for the clearance of official DoD information proposed for official public release by the Department of Defense and its employees.
- Director of Administration and Management. DoD Directive 5400.7, *DoD Freedom of Information Act (FOIA) Program*, 2 January 2008, Certified Current through 2 January 2015.  
PURPOSE: Update policies and responsibilities for implementing the DoD FOIA Program.
- Under Secretary of Defense for Research and Engineering. DoD Directive 5230.25, *Withholding of Unclassified Technical Data From Public Disclosure*, 6 November 1984, incorporating Change 1, 18 August 1995.

PURPOSE: Establish policy, prescribe procedures, and assign responsibilities for the dissemination and withholding of technical data.

- Director of Administration and Management. DoD Instruction 5122.05, *Assistant Secretary of Defense for Public Affairs*, 5 September 2008.  
PURPOSE: Define the Assistant Secretary of Defense for Public Affairs as a Principal Staff Assistant reporting directly to the Secretary of Defense, to issue DoD policy in DoD Instructions within the responsibilities, functions, and authorities pertaining to PA.
- Director of Administration and Management. DoD Instruction 5230.29, *Security and Policy Review of DoD Information for Public Release*, 8 January 2009.  
PURPOSE: Assign responsibilities and prescribe procedures to carry out security and policy review of DoD information for public release.
- Department of Defense, Research and Engineering Enterprise. DoD Instruction 3200.12, *DoD Scientific and Technical Information Program (STIP)*, 11 February 1998.  
PURPOSE: Update DoD policy and responsibilities for establishing the DoD STIP.
- Assistant Secretary of Defense for Public Affairs. DoD Instruction 5400.13, *Public Affairs Operations*, 15 October, 2008.  
PURPOSE: Establish policy and assign responsibilities for the conduct of PA as a primary DoD communications capability.
- Department of Defense, Chief Information Officer. DoD Instruction 8550.01, *DoD Internet Services and Internet-Based Capabilities*, 11 September 2012.  
PURPOSE: Establish policy, assign responsibilities, and provide instructions for establishing, operating, and maintaining DoD Internet services on unclassified networks to collect, disseminate, store, and otherwise process unclassified DoD information, and for use of Internet-based capabilities to collect, disseminate, store, and otherwise process unclassified DoD information.
- Director of Administration and Management. DoD Regulation 5400.7-R, *DoD FOIA Program*, 4 September 1998, incorporating Change 1, 11 April 2006.  
PURPOSE: Provide policies and procedures for, and promotes uniformity in, the DoD implementation of the FOIA and DoD Directive 5400.7.
- Department of Defense. DD Form 1910, *Clearance Request for Public Release of DoD Information*, January 2006.  
PURPOSE: Establish policy, prescribe procedures, and assign responsibilities for the dissemination and withholding of technical data. Copy of current form in Appendix B.
- Department of Defense, Defense Security Directorate, Office of the Under Secretary of Defense for Intelligence. *Security and Policy Reviews of Articles, Manuscripts, Books and Other Media Prior to Public Release – Frequently Asked Questions*, 2012. Available from [http://www.dtic.mil/whs/esd/osr/docs/2012SR\\_Brochure.pdf](http://www.dtic.mil/whs/esd/osr/docs/2012SR_Brochure.pdf).

PURPOSE: To provide quick reference on, and guide to the requirements of the DoD INFOSEC Program specific to submitting documents for a DoD Security and Policy Review.

### **Department of the Army**

These and other Army issuances can be found at <http://www.apd.army.mil/>.

### **Industrial Security**

- Army Regulation 380-49, *Industrial Security Program*, 20 March 2013.  
PURPOSE: Establish policy for the Army Industrial Security Program and implement policy from EO 12829, DoD 5220.22–M, DoD 5220.22–R, DoD Instruction 5220.22, and Homeland Security Presidential Directive–12.

### **Information Security**

- Army Regulation 380-5, *Department of the Army Information Security Program*, 29 September 2000.  
PURPOSE: Implement the policy set forth in EO 12958 and DoD 5200.1–R for classification, downgrading, declassification, and safeguarding of Army information requiring protection in the interest of national security.
- HQDA , G2, Memorandum Security Notice, Subject: “Standardized Methodology for Making Classification Decisions,” 25 October 2006. Available from <http://www.dami.army.pentagon.mil/site/InfoSec/Pub.aspx>.  
PURPOSE: Provide a standardized methodology for making original classification decisions to be used as a "best business practice" across the Army. Provide security managers with a tool for making original classification decisions and in developing, reviewing, or updating SCGs. Provide a standardized method of making an objective decision about a subjective issue. Create an audit trail from which to review decisions as necessary at a later date.

### **Operations Security**

- Army Regulation 530-1, *Operations Security (OPSEC)*, 19 April 2007. FOUO.  
PURPOSE: State Army OPSEC policy for program development, revise terminology, provide details on the OPSEC planning process, and outline the OPSEC review, assessment and survey. Implement DoD Directive 5205.02.

### **Public Affairs / Security and Policy Review**

- Army Regulation 360-1, *The United States Army Public Affairs Program*, 25 May 2011.  
PURPOSE: Provide guidelines for command and public information, including information released to the media, and community relations programs intended for internal and external audiences with interest in the United States Army.

## Department of the Navy

These and other Navy issuances can be found at <http://doni.daps.dla.mil/>.

### **Information and Personnel Security**

- SECNAV 5510.36A, *DON Information Security Program Instruction*, 6 October 2006.  
PURPOSE: Establish DON INFOSEC Program to observe the democratic principles of openness and the free flow of information, as well as to enforce protective measures for safeguarding information critical to national security.
- SECNAV M-5510.36, *DON Information Security Program Manual*, 30 June 2006.  
PURPOSE: Establish the DON INFOSEC Program for the classification, safeguarding, transmission and destruction of classified information. Includes requirement for Pre-Publication Security and Policy Review of information to be released to the public.
- SECNAV 5510.30B, *DON Personnel Security Program Instruction*, 6 October 2006.  
PURPOSE: Provide DON commands, activities and personnel with regulations and guidance governing the DON Personnel Security Program.
- SECNAV M-5510.30, *DON Personnel Security Program Manual*, June 2006.  
PURPOSE: Establish DON Personnel Security Program, to include roles and responsibilities for Command Security Managers.
- *DON Declassification Guide, Interagency Security Classification Appeals Panel (ISCAP) Approved*, 21 December 2012.  
PURPOSE: Detail the exemption status of 25 year old, or older, DON NSI contained in permanent historical records as required by EO 13526. This guide is the DON's authoritative source for NSI 25 years or older that is exempt from automatic declassification. The DON declassification manual contains additional subject detail to aid the declassification reviewer in the performance of their duties.
- *DON Declassification Manual*, 11 December 2012. FOUO.  
PURPOSE: Provide classification reviewers with detailed information to help them identify information in permanent historical records that is exempt from automatic declassification at 25 years. This manual is to be used in conjunction with the Interagency Security Classification Appeals Panel-approved DON Declassification Guide.

### **Operations Security**

- OPNAVINST 3432.1A, *Operations Security*, 4 August 2011.  
PURPOSE: Establish policy, procedures and responsibilities for the Navy OPSEC program. Includes "Navy OPSEC Program Management Responsibilities and Governance" as an enclosure.

## Public Affairs / Security and Policy Review

- SECNAVINST 5720.44C, *DON Public Affairs Policy and Regulations*, 21 February 2012.  
PURPOSE: Provide basic policy and regulations for carrying out the public affairs and internal relations programs of the DON. Includes provisions for Security and Policy Review.
- CHINFOINST 5720.8, *The Public Affairs Tactics Manual*, 10 June 2011.  
PURPOSE: Companion document to SECNAVINST 5720.44C; provide guidance to the Navy in the development of public affairs organizations. Includes provisions for Security and Policy Review, to include specific procedures to comply with DoD Directive 5230.9, Security and Policy Review of DoD Information for Public Release.

## United States Marine Corps

NOTE: All USMC Orders (MCO) are subordinate to the SECNAV policies listed above unless otherwise stated in the documents. These and other USMC issuances can be found at <http://www.marines.mil/News/Publications/ELECTRONICLIBRARY.aspx>.

## Information Security

- MCO P5510.18A W/Ch 1, *United States Marine Corps Information And Personnel Security Program Manual (Short Title: Marine Corps IPSP)*, 3 February 2000.  
PURPOSE: Establish the IPSP within the United States Marine Corps.
- Marine Corps Warfighting Publication (MCWP) 3-40.2, *Information Management*, 24 January 2002.  
PURPOSE: Discusses the fundamentals of information, personnel responsibilities, C2 support structure development, and security of information.

## Operations Security

- MCO 3070.2, *The Marine Corps Operations Security (OPSEC) Program*, 18 May 2007.  
PURPOSE: Publish specific instructions to Marine Corps personnel concerning OPSEC requirements and programs.

## Public Affairs / Security and Policy Review

- MCO 5230.18, *Clearance Of Department Of Defense Information For Public Release*, 10 June 1994.  
PURPOSE: Publish specific instructions to Headquarters USMC personnel and civilian employees of the USMC guiding publication of materials.
- MCO 5720.77, *Marine Corps Public Affairs Order*, 8 July 2010.  
PURPOSE: Provide updated policy and guidance for both commanding officers and PA Marines.



- MCWP 3-33.3, *Marine Corps Public Affairs*, 18 January 2000.  
PURPOSE: Describe the USMC doctrine on public affairs.

## Department of the Air Force

These and other Air Force issuances can be found at <http://www.e-publishing.af.mil>.

## **Industrial Security**

- Air Force Policy Directive 31-6, *Industrial Security*, 1 April 2000.  
PURPOSE: Provide policy for protecting classified national security and sensitive unclassified information (regardless of its classification, sensitivity, physical form, media or characteristics) and sensitive government resources entrusted to industry.
- Air Force Instruction 31-601, *Industrial Security Program Management*, 29 June 2005.  
PURPOSE: Implement AFD 31-6. Includes requirements for the Contracting Office to coordinate Industrial Security review requirements with the Security and Policy Review under Public Affairs.
- Air Force Guidance Memorandum to AFI 31-401, *Information Security Program Management*. **Currently under development.** There is an Air Force Guidance Memorandum (AFGM) that changes AFI 31-401. Compliance with the AFGM is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information in the AFGM prevails in accordance with AFI 33-360, *Publications and Forms Management*. In advance of rewrite of AFI 31-401, or publication of AFI 16-1401, *Enterprise Information Protection*, the attachment to the AFGM provides guidance changes that are effective immediately.

## **Operations Security**

- Air Force Policy Directive 10-7, *Air Force Information Operations*, 6 September 2006.  
PURPOSE: Provide guidance for planning and conducting Air Force Information Operations to support the warfighter and achieve national strategy objectives. Implements several DoD Directives, including DoD Directive 5205.05E, *DoD Operations Security (OPSEC) Program*.
- AFI 10-701, *Operations Security (OPSEC)*, 8 June 2011.  
PURPOSE: Implement AFD 10-7 by providing guidance for implementing, maintaining, and executing OPSEC programs.

## **Information Security**

- Air Force Policy Directive 31-4, *Information Security*, 1 September 1998.  
PURPOSE: Provide Air Force policy for protecting sensitive Air Force information. It also assigns responsibility for implementing and managing the INFOSEC Program.

- Air Force Instruction 31-401, *Information Security Program Management*, 1 November 2005, Incorporating Change 1, 19 August 2009.  
PURPOSE: Implement AFPD 31-4. Includes references to Security and Policy Review, as well as the responsible activity for 'Historical Researchers' and their connection to classified or sensitive information. AFHRA OL-A/HOR is the authority for granting access to historical researchers on behalf of the Air Force Historian.

### **Public Affairs / Security and Policy Review**

- Air Force Policy Directive 35-1, *Public Affairs Management*, 28 September 2012.  
PURPOSE: Establish the framework for Air Force PA operations. Mentions S&P Review process, but only as a requirement to be detailed at the AFI level. Parent policy to AFI 35-102, PA Management.
- Air Force Instruction 35-102, *Security and Policy Review Process*, 20 October 2009.  
PURPOSE: Implement AFPD 35-1, Public Affairs Management. It provides guidance for the release of accurate information that does **not** contain classified material through the S&P Review Process.

## **Information Security References, U.S. Federal Government**

### **Executive Orders**

#### *Current / In Effect*

- Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, 30 June 2008.  
PURPOSE: Amends EO 12968. Executive branch policies and procedures relating to suitability, contractor employee fitness, eligibility to hold a sensitive position, access to federally controlled facilities and information systems, and eligibility for access to classified information shall be aligned using consistent standards to the extent possible, provide for reciprocal recognition, and shall ensure cost-effective, timely, and efficient protection of the national interest, while providing fair treatment to those upon whom the Federal Government relies to conduct our Nation's business and protect national security.
- Executive Order 13526, *Classified National Security Information; Presidential Memorandum, Implementation of the Executive Order, "Classified National Security Information;" Administrative Order, "Original Classification Authority."* All dated 29 December 2009.  
PURPOSE: Revoke and replace EO 12958 and EO 13292. Directed a review of EO 12958, to include proposals concerning:
  - Establishment of a National Declassification Center;
  - Effective measures to address the problem of over classification and increase accountability for classification decisions;
  - Facilitate greater sharing of classified information;
  - Prohibition of reclassification of material that has been declassified and released to the public under proper authority;

- Consideration of the electronic environment; and
- Greater openness and transparency while also affording necessary protection to the Government's legitimate interests.

FOLLOWING PROVISIONS relate to the Implementing Memorandum for EO 13526:

- Agency implementing regulations issued in final form within 180 days of the issuance of 32 C.F.R. Part 2001 by ISOO.
  - Updates from agencies to ISOO and periodic status reports issued by ISOO.
  - Declassification of Records of Permanent Historical Value
  - Delegation of OCA
    - Shall be limited to the minimum necessary and only to those with a demonstrable and continuing need.
    - Review required with report to ISOO within 120 days of December 29, 2010 (April 28<sup>th</sup>, 2011).
  - Promotion of New Technologies to Support Declassification
    - Directs the SecDef and Director of National Intelligence to support research to assist with cross-agency challenges associated with declassification.
  - Possibility of a more fundamental transformation of the classification system.
- Executive Order 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*, 18 August 2010.  
PURPOSE: Establish a Classified National Security Information Program designed to safeguard and govern access to classified NSI shared by the Federal Government with State, local, tribal, and private sector (SLTPS) entities. Allow for access to Secret level information to SLTPS entities, and rest the determination of such access on the sponsoring agency. Possibly useful for National Historic Preservation Act consultations and, potentially, tribal consultation.
  - Executive Order 13556, *Controlled Unclassified Information*, 4 November 2010.  
PURPOSE: Establish a program for managing CUI that emphasizes the openness and uniformity of Government-wide practice. Drives DoD Manual 5200.01, Volume 4.
  - Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, 7 October 2011.  
PURPOSE: Direct structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding INFOSEC, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government.

#### *Historical / Superseded*

- Executive Order 12356, *National Security Information*, 2 April 1982.
- Executive Order 12829, *National Industrial Security Program*, 6 January 1993.

- Executive Order 12885, *Amendment to Executive Order 12829, National Industrial Security Program*, 14 December 1993.
- Executive Order 12958, *Classified National Security Information*, 20 April 1995.
- Executive Order 12968, *Access to Classified Information*, 4 August 1995.
- Executive Order 13292, *Further Amendment to Executive Order 12958, as Amended, Classified National Security Information*, 25 March 2003.

### **Information Security Oversight Office**

- 2011 Annual Report to the President, 18 May 2012. Available at: <http://www.archives.gov/isoo/reports/2011-annual-report.pdf>  
PURPOSE: Provide statistics and analysis concerning key components of the system of classification and declassification, as well as coverage of ISOO's reviews of Departments' and Agencies' programs. It also contains information with respect to industrial security in the private sector as required by EO 12829, as amended, "National Industrial Security Program."
- ISOO Notices, 2008 – Present, available from <http://www.archives.gov/isoo/notices/>.  
PURPOSE: Disseminate and provide consistent guidance to Federal Agencies, in an effort to improve their classified NSI programs. Each ISOO Notice focuses on a single topic related to classification, safeguarding, or declassification.
- Final Report for DoD's Fundamental Classification Guidance Review (FCGR), 27 June 2012. Available from <http://www.archives.gov/isoo/fcgr/dod.pdf>.  
PURPOSE: Provide a report on DoD efforts from 2011-2012 to facilitate implementation of EO 13526, Section 1.9: Fundamental Classification Guidance Review. Specifically, the Report indicates that 97% of DoD's SCGs were updated and/or declared current, and approximately 20% of DoD's non-compartmented SCGs were either eliminated or identified for retirement.

### **Information Security References, Non-Federal**

- Aerospace Industries Association. *Security and Policy Review Handbook*, Fourth Edition, 2007. Available from [http://www.aia-aerospace.org/assets/security\\_handbook\\_07.pdf](http://www.aia-aerospace.org/assets/security_handbook_07.pdf).  
PURPOSE: This handbook is a third-party (non- DoD) reference guide to submitting documents for Security and Policy Review. It includes information on the requirements, as well as the proper forms and submission protocols.
- National Classification Management Society. *A Guide for the Preparation of a DD Form 254*, no date. Available from: <https://www.classmgmt.com/>.  
PURPOSE: This guide provides preparation instructions for DD Form 254, and should be used in conjunction with DoD 5220.22-R and DoD 5220.22-M. It applies to contracting

and procurement officials, and program and project managers. All share functional industrial security program responsibilities within the Defense Information Systems Agency/Office of the Manager, National Communications System (DISA/OMNCS). The DD Form 254 is a key document in contracting actions. The form, with its attachments, supplements and incorporated references, advises contractors on the proper procedures to handle classified material received or generated under a classified contract. It identifies which security classification guidance to use, who has oversight, and where.

Intentionally Blank

# APPENDIX A: ACCESS TO CLASSIFIED INFORMATION

## ACCESS TO CLASSIFIED INFORMATION

**The time it can take to obtain a clearance can seriously affect your project schedule—this should be anticipated early and built into the project parameters.**

In order to have access to classified information a person must have a “clearance” and a “need-to-know.” The need-to-know is determined by the authorized holder of the classified information, who has been appropriately trained and follows adjudicative guidelines to make the decision to provide access. This person has the discretion to decide whether a prospective researcher truly does require access to classified information in order to “perform or assist in a lawful and authorized governmental function” and that the access is consistent with the national security interests of the U.S.<sup>116</sup>

Heads of agencies are responsible to administer a security program which includes active oversight, training, and periodic evaluations of the program administration. Employees who have been granted access to classified information must:

1. Protect classified information in their custody from unauthorized disclosure.
2. Report contact with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information.
3. Comply with all security requirements and report all violations of those requirements.
4. Report activities of fellow employees with access to classified information who “raise doubts” as to whether they are operating in a manner consistent with national security.<sup>117</sup>

### **Clearance Basics**

In order to obtain a clearance for access to classified information you must:

1. Be a U.S. citizen<sup>118</sup> who has passed a Personal Security Investigation (PSI) that shows loyalty to the U.S., strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment. Also have a willingness to follow the regulations governing the use, handling, and protection of classified information and not have a conflict of allegiances or the potential for coercion.

---

<sup>116</sup> Federal Register, Volume 60, Number 151, August 7, 1995. Presidential documents, Title 3—Executive Order 12968, “Access to Classified Information,” p.40246.

<sup>117</sup> Ibid., p. 40253.

<sup>118</sup> There are special cases where non-U.S. citizens are granted access by those who possess special expertise, but the information can only be accessed at a level that the Government has previously established for that person’s country of origin.



2. Have a demonstrated need-to-know.<sup>119</sup>
3. Have signed a non-disclosure agreement.

You may obtain clearance as a Federal employee, as long as there is a demonstrated, foreseeable need for the access; your access will be terminated when this need no longer exists. There is also a temporary access that can be granted to your contractor when they are working on a classified project. Your contractor will need to satisfy the requirements noted above and there will be a fixed date or event when the clearance will expire. The clearance will also limit the classified information to that which directly applies to the project. The level of access to classified information will also be limited by your need-to-know; it will be either confidential, secret, or top secret. If you have a higher level of access, you may also access information that is classified below that level. If you are at a lower level than required for a project, you may also be granted temporary access to higher levels: as long as there are no operational or contractual exigencies of a recurring nature that were not originally anticipated, the access will not exceed 180 days, and the access will be limited to specific information.<sup>120</sup>

Your clearance is considered “active” if it has not been terminated. Your clearance is considered “current” if you had a clearance that was terminated, but is still eligible for reinstatement, and your personnel security investigation (PSI) is not more than five years old for Top Secret, 10 years old for Secret, or 15 years old for Confidential. Your clearance is considered “expired” if you have had a break-in-service of two years or more. If this occurs and your work requires clearance, you must be nominated for a new clearance, complete a new SF 86, and undergo a new PSI. Just because you previously had an active clearance, this does not mean that you will automatically receive a new one.

Access to classified information is reciprocal to all agencies; however, outside agencies may require additional investigations and they may deny temporary access or access that has been granted as a special case (prior to full investigation).

### **Process to Obtain a Clearance**

You must be sponsored to obtain a clearance—the agency you are working with will identify you or your contractor as a person with a need to access classified information. Your agency will then send a request to the Security Officer (SO)<sup>121</sup> who will submit an investigation request through the Joint Personnel Adjudication System (JPAS). You or your contractor will then complete the SF 86 clearance application in Electronic Questionnaires for Investigations

---

<sup>119</sup> This is also required when requesting certain types of information: if you are cleared by one authorized holder, but desire information from a different authorized holder, that holder will be required to determine your need-to-know.

<sup>120</sup> Ibid., pp. 40248-40249.

<sup>121</sup> If you are a Government contractor, the request will go to your Facility Security Officer or FSO.

Processing (e-QIP) and supply fingerprints. Once the application is complete your SO will review, approve, and forward the e-QIP to the DoD Clearance Facility (DoDCAF) who will approve the request, issue an interim clearance, and release the information to the Office of Personnel Management (OPM). OPM will conduct the PSI and send the results to DoDCAF who will either grant a clearance or issue a Letter of Intent to deny the clearance.

The SF 86 in e-QIP requires personal identifying data, as well as information regarding citizenship, residence, education, and employment history; family and associates; and foreign connections / travel. You will also need to supply information about: criminal records, illegal drug involvement, financial delinquencies, mental health counseling, alcohol-related incidents and counseling, military service, prior clearances and investigations, civil court actions, misuse of computer systems, and subversive activities. The number of years of information required on the form varies from question to question—many require 7 years, some require 10 years, and others are not limited to any period of time. It is a comprehensive form to provide the Government with enough information to support your PSI.

If you are granted access to classified information, you must provide a written consent to the employing agency that you grant access to your personal information by an authorized investigative agency for the period of the clearance and an additional three years after your clearance ends. Your financial records (maintained by a financial institution), credit reports, and travel (from records maintained by commercial entities) may be investigated if there are grounds to believe that you may be disclosing classified information in an unauthorized manner to a foreign power, that you have incurred excessive debt of inexplicable affluence, or have been compromised to a foreign power.

Clearances are to be completed within 60 days, once the e-QIP is processed. However, many cases can take up to 180 days and 10% of the cases will take 6 months to over a year. As noted, *this does not include the time required to be identified as a person who should receive clearance*. The primary causes for delay are queuing time, rejection of the application, and serious security issues associated with the person requesting clearance. When the caseload is heavy for the investigators, it may take more time for your application to be reviewed. You have no control over this; however, you do have control over the information you provide on your e-QIP.

If there is missing or incorrect information on your e-QIP, the inaccuracies will be found during the PSI and your application will be rejected. If your application is rejected it could cause a delay of at least 30 to 60 days, as you will have to revise and resubmit your application; it is important to be accurate and complete when you first fill out the form, paying special attention to foreign travel, relatives, residences, addresses, telephone numbers, dates, employment, and education. You can support a quick PSI by providing the correct information on your e-QIP. However, if there is something on your e-QIP or during your PSI that the investigator determines

will require additional information or investigation, your application could be delayed for months—the delay time depends on the queue for such cases and the depth of the required additional investigation.

Things you or your contractor personnel can do to ensure a smooth process:

1. Print the form and fill it out by hand before using e-QIP.
2. Provide accurate zip codes (a typo could send your investigation to the wrong office).
3. Review your credit report and fix any issues before you submit your e-QIP.
4. Do not enter relatives in “Name of Person Who Knew You” under the residence section.
5. Obtain your fingerprints in the required 14 day time period.
6. If you have unfavorable security and suitability information<sup>122</sup>, use the terms that are directly applicable to the mitigating conditions as noted in the Adjudicative Guidelines.

### **Application Results**

Once clearance is obtained, you will be informed by your SO, receive a briefing, and be required to sign your non-disclosure agreement at that time. If your contractor’s clearance was denied, that person will receive a Letter of Intent that includes a Statement of Reasons that detail what led to the decision. At that point, the contractor can submit a written rebuttal and request a hearing; if that person does not submit a rebuttal, the request for clearance will remain denied. If the person submits a rebuttal, but does not request a hearing, an Administrative Judge will review a File of Relevant Material and make a decision based on the written record. However, if the contractor requests a hearing, that person can (with or without an attorney) present witnesses and other evidence, cross examine witnesses, and challenge DoDCAF evidence. The judge will make a decision and direct DoDCAF to grant or deny clearance based on that decision. If the contractor is still denied, that person is accorded the opportunity to appeal the judge’s decision.

Contractors have more flexibility than DoD civilian or military personnel. If you are denied, you can submit a written rebuttal, but you are not entitled to a hearing. An adjudicator will review the written information and make a decision to grant or deny. As with the private sector, you are allowed to appeal this decision.

Applicants who are denied clearance are barred from re-applying for the period of one year.

---

<sup>122</sup> Substance abuse, mental health issues, you left a job under less than favorable circumstances, financial issues, criminal conduct, etc...

## **Locating Past Results**

If you have had a clearance in the past and are unsure whether it is active or if you want to check the status of an application, this can be done through JPAS. You may also obtain a copy of a previous clearance investigation. To do this you must determine who conducted the investigation: Defense Security Service (DSS) or OPM.<sup>123</sup> The DSS PSI function transferred to OPM in 2005; if your PSI was prior to this year it is likely at DSS and if it is after it is likely that OPM retains the records. To request a DSS investigation, mail a written request with your full current name, other names you may have had, date of birth, social security number, a brief description of the records you are seeking, and other information you feel might aid in locating your record, as well as your original, notarized signature to:

Defense Security Service  
Office of FOIA and Privacy  
27130 Telegraph Road  
Quantico, VA 22134

If you want to locate OPM PSIs, you can mail or fax the request, but you will need to include your full name, social security number, date of birth, place of birth, and current home address to:

FOI/P, OPM-FIPC  
P.O. Box 618  
1137 Branchton Road  
Boyers, PA 16018-0618  
FAX: 724-794-4590

## **Company Clearance**

DISP governs the security obligations of DoD contractors and the contractors for twenty-three other agencies. The DSS has the primary responsibility for ensuring NISP compliance. In order for your company to obtain a Facility Security Clearance (FCL) it needs to be sponsored by a Federal agency (or cleared contractor to that agency) after a definite classified procurement need has been established. A DD Form 441, the agreement between the Government and the contractor, will be filled out. This form serves as the Government notification to the contractor of the classification level of information to which contractor personnel will have access and it also provides the contractor agreement that the contractor will abide by the security requirements set form in the NISP Operating Manual (NISPOM).

An FCL will also include a DD 254—this is the contracting form that is used for all contracts that include working with classified information. The form includes security classification and

---

<sup>123</sup> It is possible another agency conducted the investigation, but these two offices have completed over 90% of all PSIs.

safeguarding requirements that are required for the work. The DD 254 determines the level of FCL granted to a contractor and is required to maintain an active FCL. Any given FCL may have more than one DD 254 that guides the work being done by the contractor. Once an FCL is established, the company will be assigned an Industrial Security Representative to aid the contractor in following the requirements of the NISPOM and there will be a representative for the entire period the contractor is a NISP participant. This representative will complete periodic DSS reviews to ensure that the contractor's safeguards are adequate for the protection of classified information. This representative will also aid the FCL in determining which employees should receive clearance and will work directly with the FSO (the contractor version of the SO).

Intentionally Blank

## **APPENDIX B: STORING, HANDLING, AND TRANSMITTING INFORMATION**

## **STORING, HANDLING, AND TRANSMITTING DATA**

In addition to not releasing protected information through your publications, it is also important that the research data that may contain such information is also stored, handled, and transmitted through secure means. If your work is contracted and the Contracting Officer has included a DD 254, then the pertinent protocols will be part of the contract and your contractor will be subject to protecting the information as part of their contractual obligations.

However, should your contract not be subject to the restrictions of a DD 254 and the accompanying contractual language, and should your contractor discover information that requires protection, you should contact your ASM/CSM immediately to determine appropriate action. Alternately, during the project your ASM/CSM may discern that such information is in your contractor's possession before either of you are aware. In this case the ASM/CSM will also determine the next steps.

Below is basic information about storing, handling, and transmitting information that should aid in better understanding how to safeguard your research data and reports as they are developing. This information is excerpted from DoD guidance, so *you should check with your echelon about the specific requirements for your specific military service and your local organization*. And, if you are working with protected information on a regular basis, you should obtain training to ensure you understand all the requirements. Your ASM/CSM will know of sources for such training.

### **Protecting Data During Document Development**

Paper copies, electronic files, and other material containing classified information shall be reproduced only when necessary to accomplish your organization's mission or to comply with applicable statutes or Directives. The DoD encourages using of technology that prevents, discourages, or detects unauthorized reproduction of classified information. Unless such reproduction has been restricted by the originating agency, Top Secret, Secret, and Confidential information may be reproduced—e-mail, scan, and copy—to the extent that operational needs require. Each DoD Component has established its own procedures that facilitate the oversight and control of reproducing classified material; be sure to coordinate with the ASM/CSM in your organization to ensure you are following policy.

In addition to the information in your final report and known copies of classified material, you will need to protect the data that was used to develop the document. This information is referred to as “working papers.” Working papers are documents—such as notes, drafts, prototypes—or materials—such as printer ribbons and photographic plates—regardless of the media, created during development and preparation of a finished product. Working papers and materials are not intended or expected to be disseminated; in cultural resources these would include notes, copies, draft documents, and other research data used to generate your final report. Working papers



need to be marked as such and safeguarded as classified material. For more information on the specific treatment of these materials see DoD Manual 5200.01, Volume 3, Enclosure 2.

## **Equipment**

When working with classified data it is important to use DoD communication security-approved equipment, including copiers, facsimile machines, computers and other IT equipment and peripherals, display systems, and electronic typewriters. Your organization will have protocols with regard to approved equipment as well as the potential use of non-communication security-approved equipment; which is viable to use as long as the proper protections are in place. If you are using a computer for classified data it must be certified and accredited in accordance with DoD Directive 8500.01E, *Information Assurance*. The measures that must be in place to protect against compromising emanations are implemented in accordance with DoD Directive C-5200.19, *Control of Compromising Emanations*.

## **Communications**

In accordance with the requirements of DoD Manual 5200.01, Volume 3 Enclosure 4, classified information can only be transmitted over secure communications lines that have been approved for transmission of information at the specified level of classification. This includes communication by telephone, facsimile, e-mail and other forms of electronic communications, including messaging, websites, and file transfer sites.

Classified data cannot be posted to the Internet. Also, FOUO and other CUI cannot be posted to publicly-accessible Internet sites or to sites whose access is controlled only by domain—such as .mil and / or .gov. Even though these can provide restricted access, such access can easily be circumvented. At a minimum, posting CUI to a website requires common access card (certificate-based) or password and ID access as well as encrypted transmission using hypertext transfer protocol secure (https) or similar technology. It is important to note that CUI other than FOUO may have additional posting restrictions.

Only the top positions in the DoD or DoD Components are allowed to take protected information from designated work places to work at home.

## **Storing Information**

Classified information is to be secured under conditions that are adequate to deter and detect access by unauthorized persons. Holdings of classified material should be reduced to the minimum required to accomplish the mission. As historians we are prone to collecting everything and anything that may bear on our topic, but if you are working with classified information it would be better to collect only that which is directly and absolutely pertinent to the topic of your research. The research data you collect must be stored in a proper container that is always closed and locked when not in use.

GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for storing and protecting classified information. GSA-approved security containers must have a label stating “General Services Administration Approved Security Container,” affixed to the front of the container, usually on the control or the top drawer. Your organization will have lock, intrusion detection systems, and other security requirements you may need to understand. Classified data has higher protection requirements than CUI—see DoD Manual 5200.01, Volume 3 and Volume 4 for more detailed information.

### **Handling Information**

If you are working with classified material that you have removed from storage, you are required to keep it under constant surveillance. Classified document cover sheets (SF 703, “Top Secret (Cover sheet);” SF 704, “Secret (Cover sheet);” or SF 705 “Confidential (Cover sheet)”) shall be placed on classified documents not in secure storage. The cover sheets show, by color and other immediately recognizable format or legend, the applicable classification level.

The heads of your organization will have established a system of security checks that are to be implemented at the close of each duty and / or business day to ensure that any area where classified information is used or stored is secure. The SF 701, “Activity Security Checklist,” will be used to record such checks. An integral part of the security check system shall be the securing of all vaults, secure rooms, and containers used for storing classified material, which is recorded on a SF 702, “Security Container Check Sheet.”

### **Data Spills**

A data spill can occur when you are e-mailing files to your contractor or someone within your organization for review.

Classified data spills occur when classified data is introduced either onto an unclassified information system or to an information system with a lower level of classification, or to a system not accredited to process data of that restrictive category. Although it is possible that no unauthorized disclosure occurred, classified data spills are considered and handled as a possible compromise of classified information involving information systems, networks, and computer equipment until the inquiry determines whether an unauthorized disclosure did or did not occur.<sup>124</sup>

When a classified data spill occurs, your ASM/CSM will be responsible for ensuring that the policy requirements for addressing an unauthorized disclosure are met (e.g., inquiry, notification, investigation, damage assessment). The ASM/CSM has the lead, but will consult closely with your IT and / or IA staff, which has overall responsibility for the operation of the networks and systems as well as the technical knowledge needed to address the spill. If your electronic media

---

<sup>124</sup> DoD Manual 5200.01, Volume 3, Enclosure 7. p. 104.

is involved, 1) there will be a prompt and coordinated response; 2) your media will become classified at the same level as the spilled information; and 3) mitigation—such as sanitization, physical removal, or destruction—will be considered. Your system will be isolated and the hardware has the potential to be destroyed, although it is likely for a cultural resource spill that the drive could be sanitized and overwritten; however, although your drive may be overwritten, it could remain at the higher classified level, which would require providing a new system for you.

## **Destruction**

When your project is complete you will either be returning information to the original source or be required to destroy your copies. Classified documents and material identified for destruction are to continue to be protected at their classification level until they are destroyed. They are to be destroyed completely by appropriately cleared personnel to prevent anyone from reconstructing the classified information; when destroying documents you will need to follow the procedures and methods that your DoD Component Head has prescribed.

Methods and equipment used to routinely destroy classified information include burning, crosscut shredding, wet pulping, mutilation, chemical decomposition or pulverizing. Methods used for clearing, sanitization or destruction of classified IT equipment and media include overwriting, degaussing, sanding, and physical destruction of components or media. Only equipment listed on an evaluated products list (EPL) that has been issued by National Security Administration may be used to destroy classified information using any method covered by an EPL. EPLs currently exist for paper shredders, punched tape destruction devices, optical media destruction devices (for compact discs (CDs) and digital video discs (DVDs)), degaussers (for magnetic media sanitization), and disintegrators (for paper and punched tape material). The EPLs may be obtained at [http://www.nsa.gov/ia/guidance/media\\_destruction\\_guidance/index.shtml](http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml).

You may use equipment that was approved for use prior to January 1, 2011 that is not found on the appropriate EPL until December 31, 2016. And, unless determined otherwise by NSA, whenever an EPL is revised, equipment removed from the EPL may be utilized for destruction of classified information for up to 6 years from the date of its removal from the EPL.

Classified IT storage media, such as hard drives, cannot be declassified by overwriting. Sanitization (which may destroy the usefulness of the media) or physical destruction is required for disposal.

## **Transmitting Information**

If you have access to a secure e-mail, then using electronic computer-to-computer means is the preferred method of transmitting information. If not, then you will need to obtain a hand-carry authorization or use regular mail.

## **Electronically**

The only method approved for transmitting classified information is the DoD's SIPRNET (Secret Internet Protocol Router Network). If you only have access to NIPRNET (Non-classified Internet Protocol Router Network) then you may not transmit information electronically; however, if your organization allows for FOUO to be transmitted on NIPRNET, you can use e-mail for this.

- In order to have access to the SIPRNET you must have a SECRET security clearance and an authorized password
- If you have access to the SIPRNET then you are in a position to transmit classified information via a secure mode, as long as the information is marked as required.

## **Secure Facsimile**

You may use a facsimile machine to transmit information if it is a secure facsimile unit. In order to do so you will need to:

- Follow the encryption procedures for that equipment.
- Prior to transmitting, call the receiving office to ensure an authorized person is available to receive the transmission.
- Remain with the unit until the transmission or reception is complete.

## **Postal Service**

This method of transmission is not commonly used by those who work regularly with classified material, because they have authorized computers and email to transmit classified information. However, you may not have access to such technology and may need to rely on regular mail. If you need to mail classified information contact your ASM/CSM for guidance. However, some basic parameters are listed below:

- Top Secret can only be sent via courier
- Secret/Confidential can be sent via:
  - USPS Registered to U.S., Puerto Rico, U.S. Territories, and also outside of territories if they are in U.S. control (i.e. FPO or APO).
  - USPS Express Mail to U.S. and Puerto Rico.
  - Small Package Carrier, such as FedEx and UPS to U.S. and Puerto Rico only.
- You must protect unopened registered, certified, first class (return services requested), and express mail AS CLASSIFIED MATERIAL

Before sending information you must prepare package to minimize risk of accidental exposure or compromise and facilitate the detection of unauthorized tampering by placing coversheets on the front and back of to identify the overall classification and prevent ink transfer. For the

coversheets, you will need to use SF 704 – SECRET or SF 705 – CONFIDENTIAL, then wrap with plain brown paper (preferred), and seal with paper tape on all seams. You will need to include the full address, individual's name, and markings on the inner wrapper and just the full address on the outer.

If you receive a secured package it should go directly to the addressee or into the proper storage immediately. It should never be put into office routing or left unattended on a desk.

### **Hand-carry**

You may hand carry information with an authorization from Unit Commander, Staff Agency Chief, or ASM/CSM. Your ASM/CSM or supervisor will brief the authorized member carrying the classified material prior to departure; never hand-carry classified information until you have been briefed. To hand-carry information you will need a DD 2501, Carrier Authorization that was issued by your ASM/CSM. Exceptions to this may include transmitting information between offices within a secure installation, leased facilities, or office in the local commuting area or using a courier authorization letter for infrequent courier situations. Hand-carrying is not allowed on commercial flights.

### **Conversation**

You may use STU/STE (secure telephone unit/secure terminal equipment) for verbal discussions about classified information. You will need to:

- Consult with your ASM/CSM before use.
- Follow the encryption procedures for the equipment.
- Ensure other people are not within hearing range of your voice.

### **Security Incidents**

If you discover or have inadvertently caused a security incident it is important to report it immediately. Prompt reporting of such incidents ensure that they are properly investigated and the necessary actions are taken to negate or minimize the adverse effects of an actual loss or unauthorized disclosure of classified information. It can also aid in avoiding a recurrence through an informed, properly tailored, and up-to-date security education and awareness program. In cases where there is an investigation and compromise has been ruled out—there is no adverse effect on national security—a common-sense approach to the early resolution of the incident at the lowest appropriate level should take place. However, all security incidents involving classified information will involve a security inquiry, a security investigation, or both.

If there is an incident the following are the potential results:

1. **Infraction.** An infraction is a security incident involving failure to comply with requirements which cannot reasonably be expected to, and does not, result in the loss,

suspected compromise, or compromise of classified information. An infraction may be unintentional or inadvertent. While it does not constitute a security violation, if left uncorrected, can lead to security violations or compromises. It requires an inquiry to facilitate immediate corrective action but does not require an in-depth investigation.

2. **Violation.** Violations are security incidents that indicate knowing, willful, and negligent for security regulations, and result in, or could be expected to result in, the loss or compromise of classified information. Security violations require an inquiry and/or investigation.
  - a. **Compromise.** A compromise is a security incident (more specifically, a violation) in which there is an unauthorized disclosure of classified information (i.e., disclosure to a person(s) who does not have a valid clearance, authorized access, or a need to know).
  - b. **Loss.** A loss occurs when classified information cannot be physically located or accounted for (e.g., classified information/equipment is discovered missing during an audit and cannot be immediately located).
3. **Inquiry.** An inquiry is fact-finding and analysis conducted to determine whether or not there was a loss of classified information or whether or not unauthorized personnel had, or could have had, access to the information. The inquiry identifies the facts, characterizes the incident as an infraction or a violation, identifies if possible the cause(s) and person(s) responsible, reports corrective actions taken or to be taken, and makes recommendations as to the need for further corrective action or a more in-depth investigation. Inquiries, generally, are initiated and conducted at the lowest echelon possible within the DoD Component.
4. **Investigation.** An investigation is conducted for a security violation when the incident cannot be resolved via inquiry or for incidents where an in-depth and comprehensive examination of the matter is appropriate.<sup>125</sup>

## **Consequences**

If the conclusion of the investigation is that the incident was the result of a larger procedural or DoD policy weakness or vulnerability, the appropriate responsible security official will take prompt action to issue new or revised guidance, as necessary, to resolve identified deficiencies. Results of inquiries and/or investigations into actual or potential compromises that indicate that defects in the procedures and requirements of DoD Manual 5200.01 contributed to the incident shall be reported to the Director of Security, OUSD(I).

---

<sup>125</sup> DoD Manual 5200.01, Volume 3, Enclosure 6. Pp. 84-85.

If the conclusion of the investigation is that a compromise did not occur, but that there was potential for compromise of classified information due to a failure of you, your contractor, or a combination of personnel to comply with established security practices and / or procedures, the official having security responsibility over those involved will be responsible to take the appropriate action necessary to resolve the incident.

Additional investigation may be needed to permit the application of appropriate sanctions for the violation of regulations, criminal prosecution, or to develop effective remedies for the discovered vulnerabilities. If there is additional investigation, the OCAs will be notified promptly that there was a compromise and that the investigation is ongoing. The OCA will also evaluate the information and whether it has lost sensitivity since it was first classified, whether the information has been so compromised maintaining its classification is unrealistic, and the damage effect of the compromise has on the classified program and whether countermeasures can be put into effect.

Intentionally Blank



## **APPENDIX C: FORMS**

**DD 254: Contract Security Classification Specification**

**DD 1910: Clearance Request for Public Release of DoD Information**

**SF 298: Report Documentation Page**

<b>DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION</b> <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				<b>1. CLEARANCE AND SAFEGUARDING</b> a. FACILITY CLEARANCE REQUIRED  b. LEVEL OF SAFEGUARDING REQUIRED																																																																																							
<b>2. THIS SPECIFICATION IS FOR:</b> <i>(X and complete as applicable)</i>				<b>3. THIS SPECIFICATION IS:</b> <i>(X and complete as applicable)</i>																																																																																							
a. PRIME CONTRACT NUMBER				a. ORIGINAL <i>(Complete date in all cases)</i>		DATE (YYYYMMDD)																																																																																					
b. SUBCONTRACT NUMBER				b. REVISED <i>(Supersedes all previous specs)</i>		REVISION NO. DATE (YYYYMMDD)																																																																																					
c. SOLICITATION OR OTHER NUMBER		DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete Item 5 in all cases)</i>		DATE (YYYYMMDD)																																																																																					
<b>4. IS THIS A FOLLOW-ON CONTRACT?</b> <input type="checkbox"/> YES <input type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.																																																																																											
<b>5. IS THIS A FINAL DD FORM 254?</b> <input type="checkbox"/> YES <input type="checkbox"/> NO. If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.																																																																																											
<b>6. CONTRACTOR</b> <i>(Include Commercial and Government Entity (CAGE) Code)</i>																																																																																											
a. NAME, ADDRESS, AND ZIP CODE				b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>																																																																																					
<b>7. SUBCONTRACTOR</b>																																																																																											
a. NAME, ADDRESS, AND ZIP CODE				b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>																																																																																					
<b>8. ACTUAL PERFORMANCE</b>																																																																																											
a. LOCATION				b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>																																																																																					
<b>9. GENERAL IDENTIFICATION OF THIS PROCUREMENT</b>																																																																																											
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%;">10. CONTRACTOR WILL REQUIRE ACCESS TO:</th> <th style="width: 5%;">YES</th> <th style="width: 5%;">NO</th> <th style="width: 60%;">11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</th> <th style="width: 5%;">YES</th> <th style="width: 5%;">NO</th> </tr> </thead> <tbody> <tr> <td>a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION</td> <td></td> <td></td> <td>a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY</td> <td></td> <td></td> </tr> <tr> <td>b. RESTRICTED DATA</td> <td></td> <td></td> <td>b. RECEIVE CLASSIFIED DOCUMENTS ONLY</td> <td></td> <td></td> </tr> <tr> <td>c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION</td> <td></td> <td></td> <td>c. RECEIVE AND GENERATE CLASSIFIED MATERIAL</td> <td></td> <td></td> </tr> <tr> <td>d. FORMERLY RESTRICTED DATA</td> <td></td> <td></td> <td>d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE</td> <td></td> <td></td> </tr> <tr> <td>e. INTELLIGENCE INFORMATION</td> <td></td> <td></td> <td>e. PERFORM SERVICES ONLY</td> <td></td> <td></td> </tr> <tr> <td>(1) Sensitive Compartmented Information (SCI)</td> <td></td> <td></td> <td>f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES</td> <td></td> <td></td> </tr> <tr> <td>(2) Non-SCI</td> <td></td> <td></td> <td>g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER</td> <td></td> <td></td> </tr> <tr> <td>f. SPECIAL ACCESS INFORMATION</td> <td></td> <td></td> <td>h. REQUIRE A COMSEC ACCOUNT</td> <td></td> <td></td> </tr> <tr> <td>g. NATO INFORMATION</td> <td></td> <td></td> <td>i. HAVE TEMPEST REQUIREMENTS</td> <td></td> <td></td> </tr> <tr> <td>h. FOREIGN GOVERNMENT INFORMATION</td> <td></td> <td></td> <td>j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS</td> <td></td> <td></td> </tr> <tr> <td>i. LIMITED DISSEMINATION INFORMATION</td> <td></td> <td></td> <td>k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE</td> <td></td> <td></td> </tr> <tr> <td>j. FOR OFFICIAL USE ONLY INFORMATION</td> <td></td> <td></td> <td>l. OTHER <i>(Specify)</i></td> <td></td> <td></td> </tr> <tr> <td>k. OTHER <i>(Specify)</i></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>								10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO	a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION			a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY			b. RESTRICTED DATA			b. RECEIVE CLASSIFIED DOCUMENTS ONLY			c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			c. RECEIVE AND GENERATE CLASSIFIED MATERIAL			d. FORMERLY RESTRICTED DATA			d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE			e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY			(1) Sensitive Compartmented Information (SCI)			f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES			(2) Non-SCI			g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER			f. SPECIAL ACCESS INFORMATION			h. REQUIRE A COMSEC ACCOUNT			g. NATO INFORMATION			i. HAVE TEMPEST REQUIREMENTS			h. FOREIGN GOVERNMENT INFORMATION			j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS			i. LIMITED DISSEMINATION INFORMATION			k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE			j. FOR OFFICIAL USE ONLY INFORMATION			l. OTHER <i>(Specify)</i>			k. OTHER <i>(Specify)</i>					
10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO																																																																																						
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION			a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY																																																																																								
b. RESTRICTED DATA			b. RECEIVE CLASSIFIED DOCUMENTS ONLY																																																																																								
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			c. RECEIVE AND GENERATE CLASSIFIED MATERIAL																																																																																								
d. FORMERLY RESTRICTED DATA			d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE																																																																																								
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY																																																																																								
(1) Sensitive Compartmented Information (SCI)			f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES																																																																																								
(2) Non-SCI			g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER																																																																																								
f. SPECIAL ACCESS INFORMATION			h. REQUIRE A COMSEC ACCOUNT																																																																																								
g. NATO INFORMATION			i. HAVE TEMPEST REQUIREMENTS																																																																																								
h. FOREIGN GOVERNMENT INFORMATION			j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS																																																																																								
i. LIMITED DISSEMINATION INFORMATION			k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE																																																																																								
j. FOR OFFICIAL USE ONLY INFORMATION			l. OTHER <i>(Specify)</i>																																																																																								
k. OTHER <i>(Specify)</i>																																																																																											

DD FORM 254, DEC 1999

PREVIOUS EDITION IS OBSOLETE.

Reset Adobe Professional 7.0

**12. PUBLIC RELEASE.** Any information (*classified or unclassified*) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release  Direct  Through (*Specify*)

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)\* for review.  
 \*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

**13. SECURITY GUIDANCE.** The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (*Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*)

**14. ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to ISM requirements, are established for this contract.  Yes  No  
 (*If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.*)

**15. INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office.  Yes  No  
 (*If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.*)

**16. CERTIFICATION AND SIGNATURE.** Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE ( <i>Include Area Code</i> )
d. ADDRESS ( <i>Include Zip Code</i> )	<b>17. REQUIRED DISTRIBUTION</b> <input type="checkbox"/> a. CONTRACTOR <input type="checkbox"/> b. SUBCONTRACTOR <input type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input type="checkbox"/> f. OTHERS AS NECESSARY	
e. SIGNATURE		

DD FORM 254 (BACK), DEC 1999

Reset

CLEARANCE REQUEST FOR PUBLIC RELEASE OF DEPARTMENT OF DEFENSE INFORMATION		
<i>(See Instructions on back.)</i>		
<i>(This form is to be used in requesting review and clearance of DoD information proposed for public release in accordance with DoDD 5230.09.)</i>		
<b>TO: (See Note) Chief, Office of Security Review, 1155 Defense Pentagon, Washington, DC 20301-1155</b>		
Note: Regular mail address shown above. For drop-off/next day delivery, use: Room 12047, 1777 North Kent Street, Rosslyn, VA 22209-2133		
<b>1. DOCUMENT DESCRIPTION</b>		
a. TYPE	b. TITLE	
c. PAGE COUNT	d. SUBJECT AREA	
<b>2. AUTHOR/SPEAKER</b>		
a. NAME <i>(Last, First, Middle Initial)</i>	b. RANK	c. TITLE
d. OFFICE		e. AGENCY
<b>3. PRESENTATION/PUBLICATION DATA</b> <i>(Date, Place, Event)</i>		
<b>4. POINT OF CONTACT</b>		
a. NAME <i>(Last, First, Middle Initial)</i>		b. TELEPHONE NO. <i>(Include Area Code)</i>
<b>5. PRIOR COORDINATION</b>		
a. NAME <i>(Last, First, Middle Initial)</i>	b. OFFICE/AGENCY	c. TELEPHONE NO. <i>(Include Area Code)</i>
<b>6. REMARKS</b>		
<b>7. RECOMMENDATION OF SUBMITTING OFFICE/AGENCY</b>		
a. THE ATTACHED MATERIAL HAS DEPARTMENT/OFFICE/AGENCY APPROVAL FOR PUBLIC RELEASE <i>(qualifications, if any, are indicated in Remarks section)</i> AND CLEARANCE FOR OPEN PUBLICATION IS RECOMMENDED UNDER PROVISIONS OF DODD 5230.09. I AM AUTHORIZED TO MAKE THIS RECOMMENDATION FOR RELEASE ON BEHALF OF:		
_____		
b. CLEARANCE IS REQUESTED BY _____ <i>(YYYYMMDD)</i> .		
c. NAME <i>(Last, First, Middle Initial)</i>	d. TITLE	
e. OFFICE	f. AGENCY	
g. SIGNATURE		h. DATE SIGNED <i>(YYYYMMDD)</i>

DD FORM 1910, JAN 2006

PREVIOUS EDITION MAY BE USED.

Reset

Adobe Professional 8.0

## INSTRUCTIONS

**GENERAL NOTE FOR PERSONNEL PROCESSING THIS REPORT:** Items marked with an asterisk (\*) have been registered in the DoD Data Element Program.

**1. DOCUMENT DESCRIPTION.**

a. Type - Record nature of material submitted; e.g., speech, article, manuscript, study/thesis, brochure, news release, advertisement, radio/television script, etc.

b. Title - Record the exact caption, headline, name or label of the material.

c. Page Count - Enter the number of pages of the document submitted.

d. Subject Area - Record major topic or theme, whenever possible.

Examples: "Go-Between Circuits III - Total Force in Action," and "Communications."

**2. AUTHOR/SPEAKER.**

\*a. Name - Self explanatory.

\*b. Rank - Self explanatory.

c. Title - Self explanatory.

d. Office - Self explanatory.

e. Agency - Self explanatory.

**3. PRESENTATION/PUBLICATION DATA.** Record the forum of open presentation or publication.

**4. POINT OF CONTACT**

\*a. Name - Self explanatory.

b. Telephone Number - Enter the office phone number of the point of contact.

**5. PRIOR COORDINATION.** Self explanatory.

**6. REMARKS.** Enter any additional pertinent information.

**7. RECOMMENDATION OF SUBMITTING OFFICE/AGENCY.** It is of paramount importance to components, as large and complex as those which comprise the Department of Defense, that coordinated and consistent security and policy determinations are made; therefore, Item 7 must be completed by an individual who possesses the authority to communicate a particular component's policies and recommendation.

a. Enter title of Component/Agency Head or title of other individual ultimately responsible for the substantive issues addressed.

Examples: Secretary of the Army; Chairman of the Joint Chiefs of Staff; President, National Defense University; etc.

\*b. Clearance is requested by - Self explanatory.

\*c. Name - Entry must be typed or printed and coincide with signatory official.

d. Title - Self explanatory.

e. Office - Self explanatory.

f. Agency - Self explanatory.

g. Signature - Mandatory.

\*h. Date - Self explanatory.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188		
<small>Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</small>					
1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION / AVAILABILITY STATEMENT					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (include area code)

Standard Form 298 (Rev. 8-98)  
Prescribed by ANSI Std. Z39.18

## **APPENDIX D: NON-DISCLOSURE EXAMPLE FROM DD 254 ATTACHMENT**

## Attachment 1 to the DD Form 254. DUSD (AT&amp;L) Requirements for DoD Contractors

Continuation for Block 13, DD Form 254 for contract number: \_\_\_\_\_

**Period of Performance:**

1. **General:** This contract involves varying levels of classified access and clearance requirements based on individual office and mission requirements. Contractors shall follow all applicable Standard Office Procedures.
  - a. All contractor personnel performing under this contract shall possess a minimum of an interim Secret clearance, unless specified as requiring a higher level clearance, prior to reporting to any assignment within ODUSD (AT&L).
  - b. Following the major heading below there are variable provisions, which the applicability is indicated by a block marked by the COR/CM as applicable or not applicable as appropriate to this contract. Provisions not containing this variable indicating not applicable will apply in all cases to performance of this contract.
  - c. Prior approval of the contracting activity and concurrence of the COR/CM is required for any subcontracting.
  - d. The use of cellular phones, hand-held radios, beepers, pagers, cordless phones, and cordless microphones shall be addressed in the Standard Operating Procedures of each computer facility where classified information processing is accomplished.
  - e. All contractor personnel performing under this contract shall be required to sign and execute a proprietary information non-disclosure statement. The proprietary information non-disclosure statement shall be required as part of the initial in-processing and must be executed prior to performing any work under this contract. The proprietary information non-disclosure will be maintained on file within the AT&L Security Office. Contractor personnel who refuse to sign the proprietary information non-disclosure statement will not be permitted to work within AT&L. Procedures and requirements for handling Sensitive But Unclassified (which includes Proprietary Information) are contained at Attachment 5.
2. **Top Secret Clearance.** (*Item 1a must be marked Top Secret for this to apply*) Specified positions designated by the Contracting Officers Representative (COR) or Contract Monitor (CM) will require a Top Secret clearance
 

\_\_\_\_\_ Applicable                        X   Not Applicable.
3. **Actual Performance.** (*Item 8a must be marked "See Item 13" and applies if 11a is marked yes*) Contractor performance is restricted 4800 Mark Center Drive, Alexandria, VA 22350. Attend meetings in NCR.
4. **COMSEC information.** (*Applies if block 10a is marked yes*) The contractor will require administrative access to classified COMSEC material and may be required to serve as alternate COMSEC Receipt Holder. The contractor will not receipt, copy, or generate classified COMSEC material unless specifically authorized in writing by the COR or CM. The contractor must forward any request for COMSEC material/information through the government program manager to the COMSEC Manager. Access to COMSEC is restricted to US citizens holding a final US Government clearance. Such information is not releasable to personnel holding a reciprocal clearance. Access to COMSEC information at the contractor facility requires establishment of a COMSEC account. Contractor will coordinate with the Defense Security Service and the NSA Central Office of Record. Contractor is responsible for accountable COMSEC information and must provide a complete inventory as required by the COMSEC manager. Clearances appropriate to the equipment classification level is required. COMSEC briefings will be provided by the government. COMSEC



material/information may not be released to DoD contractors without OSD Program Managers approval. Contractor must forward requests for COMSEC material/information to the COMSEC officer through the program office. Contractor complies with NSA Manual 3-16 (U) in the control and protection of COMSEC material/information. Access to COMSEC material is restricted to U.S. citizens holding final U.S. Government clearances. Such information will not be released to personnel holding only reciprocal clearances.

Applicable  Not Applicable.

5. **Restricted Data.** (*Applies if block 10b is marked yes*) Access to RESTRICTED DATA, information which is classified and controlled under the Atomic Energy Act of 1954, or CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) is required. A final U.S. Government Top Secret clearance is required for this project. Information in this category relates to: (1) the design, manufacture or utilization of atomic weapons, (2) the production of special nuclear material; or, (3) the use of special nuclear material in the production of energy. Information of this category shall not be disseminated outside official and authorized channels without the consent of the originator. Access to and dissemination of this information shall be governed by DoD Instruction 5230.23 and DoD Directive C-5230.23.

Applicable  Not Applicable.

6. **CNWDI Information.** (*Applies if 10c is yes*) Contract personnel are permitted access to CNWDI in the performance of this contract. The government program manager or designated representative will brief all contractors prior to granting access to CNWDI information. Contractor must be briefed by at appropriate government agent and follow the guidelines as outline in DoD Directive 5210.2. Restricted Data shall be handled in accordance with the applicable guidance for Nuclear Weapons (Secret/RD)

Applicable  Not Applicable.

7. **Formerly Restricted Data.** (*Applies if block 10d is marked yes*) Information that is removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For Foreign Dissemination however, it is treated in the same manner as Restricted Data. Information of this category shall not be disseminated outside official channels without the consent of the originator. Access to and dissemination of this information shall be governed by DoD Instruction 5230.23 and DoD Directive C-5230.23. Access to FORMERLY RESTRICTED DATA requires a final U.S. Government clearance at the Top Secret level.

Applicable  Not Applicable.

8. **SCI Requirement.** (*Applies if 10e(1) is yes*) Performance requiring access to or at the SCI level shall be governed by the SCI addendum titled **“Release Of Sensitive Compartmented Information (SCI) Intelligence Information To Us Contractors”**. Prior approval of contracting activity is required for subcontracting. Access to Intelligence information requires SCI indoctrination and a final Top Secret U.S. Government clearance. Contractor will require access to DCID 6/9 and DCID 6/6. The names of contractor personnel requiring access to SCI shall be submitted to the contracting officer's representative (COR) for approval. The COR will approve and coordinate visits by contractor personnel to insure satisfactory justification.

Applicable  Not Applicable.

9. **Non SCI Intelligence.** (*Applies if 10e(2) is yes*) Performance requiring access to Non-SCI intelligence information shall be governed by the addendum titled **“Release of Non-SCI Intelligence Information to DoD Contractors”** Contractor will require access to DCID 6/5.

Applicable  Not Applicable.

**10. Special Access Provisions Apply.** (*Applies if block 10f is marked yes*) Contract requires access to Special Access Programs. Security guidance for operating procedures will be provided under separate cover. All SAP material remains the property of the releasing Government User Agency. Upon completion or cancellation of this contract, SAP materials previously furnished will be returned to the direct custody of Director, AT&L SAPCO, to include final reports produced at the SAP level. The SAP Program Manager will provide security classification guidance for the performance of the contract. Contractor personnel must adhere to the special access requirements/procedures developed by the SAP program/study manager. User agency managers will grant access when the need-to-know is established and required to accomplish the required efforts under this contract. SAP program/study manager must approve all requests for access. See Special Access Requirements/Procedures attachment for additional guidance.

Applicable  Not Applicable.

**11. NATO Information.** (*Applies if block 10g is marked yes*) The contractor is permitted access to North Atlantic Treaty Organization (NATO) information in performance of this contract. The government project manager is the designated representative that will ensure the Contractor Facility Security Officer (FSO) and concerned employees are NATO briefed prior to access being granted. The Prime contractor must receive approval from the Government Contracting Authority (GCA) to grant NATO accesses to a subcontractor. Access requires a final US Government clearance at the appropriate level. Forward NATO classified materials needed by the contractor only from a Service Sub-registry directly to the contractor concerned. Special briefings are required for access to NATO information. Prior approval of the government program manager is required for subcontracting. Access to NATO information requires a FINAL U.S. Government clearance at the appropriate level and special briefings. Individuals must have a briefing in accordance with United States Security Authority for NATO (USSAN) Affairs Instruction 1-69 (5100.55 Enclosure 2), "United States Implementation of NATO Security Procedures", Section VI. The briefing ensures individuals with access to NATO information are aware of pertinent security regulations for safeguarding NATO classified information and the consequences of negligent handling. The use of the Central U.S. Registry (CUSR) is mandated for receiving and transferring NATO materials. The Government Contracting Activity must authorize the hand-carrying of NATO classified material across international borders. This will only be authorized when urgent situation exists. Designated couriers must have a NATO Courier Certificate. Access to the Joint Staff Information Network (JSIN-C) requires the individual to be cleared for NATO Secret. Within 30 days of arrival at the Joint Staff, the contractor is required to attend the Security Indoctrination Blocks of the Joint Staff Training Program, if they have not previously attended. The contractor is not authorized to destroy controlled classified material.

Applicable  Not Applicable.

**12. Foreign Government Information.** (*Applies if block 10h is marked yes*) The contractor is permitted access to Foreign Government Information in the performance of this contract. Access to Foreign Government Information requires a US Government clearance at the appropriate level. Comply with the Foreign Government information requirements in the NISPOM, Chapter 10, section 3.

Applicable  Not Applicable.

**13. FOUO Information.** (*Applies if block 10j is marked yes*) Performance requiring access to For Official Use Only information (FOUO) shall be governed by the addendum titled **“For Official Use Only Addendum to DoD Contractors”**

Applicable  Not Applicable.

**14. Performance in Government Facilities.** (Mark block 10k yes and reference AT&L attachment 1 for specifics) This contract requires personnel to perform work as a member of, or in direct support of, the AT&L staff and will require individuals to work within Government controlled facilities. All contractor personnel under this contract who have access to classified information must possess a final U.S. SECRET clearance. The Contract Monitor will provide security classification guidance for the performance of this contract. AT&L will provide security classification guidance for the performance of this contract.

Applicable  Not Applicable.

- a. In and Out Processing This contract requires personnel to perform work as a member of, or in direct support of, the AT&L staff and will require individuals to obtain and maintain government issued building access cards to enable performance within Government controlled facilities. As such, all contractor personnel are required to in-process with the Administration Directorate prior to reporting for work. As a condition of this contract, all personnel issued government access cards are required to ensure the card is returned to the AT&L Security office upon removal from the contract or termination of employment under this contract. Applies in all cases where paragraph 14 above is marked applicable.
- b. Escape Mask Program. This contract requires personnel to perform work as a member of, or in direct support of, the AT&L staff and will require individuals to obtain and maintain government furnished escape masks to enable performance within Government controlled facilities. As such, all contractor personnel are required to in-process with the Administration Directorate Escape Mask Coordinator immediately (within 24 hours) of reporting for work. As a condition of this contract, all personnel issued government escape masks are required to ensure the mask is returned to the AT&L Escape Mask coordinator upon removal from the contract or termination of employment under this contract. Applies in all cases where paragraph 14 above is marked applicable.

**15. Common Access Cards.** This contract requires personnel to obtain the Government issued Common Access Card in order to provide identification or to access government computer systems. As such, all contractor personnel are required to in-process with the Administration Directorate Badge and CAC Coordinator immediately (within 24 hours) of reporting for work. As a condition of this contract, all personnel issued Government Common Access Cards are required to ensure the card is returned to the AT&L Security Office or the CAC Coordinator upon removal from the contract or termination of employment under this contract.

Applicable  Not Applicable.

**16. NIPRNET access required.** (Mark block 10k yes and reference AT&L attachment 1 for specifics) This contract requires the contractor to access and use the Unclassified government computer system known as the NIPRNET at locations identified by the government customer. All provisions of DoD Information Technology Security Certification and Accreditation Process (DITSCAP) apply. This system is Unclassified only, and inappropriate or improper use of the system will result in a reportable incident to the Defense Security Service.

Applicable  Not Applicable.

**17. SIPRNET access required.** (Mark block 10k yes and reference AT&L attachment 1 for specifics) This contract requires the contractor to access and use the Classified government computer system known as the SIPRNET at locations identified by the government customer. All provisions of DoDI 8510.01. DoD Information Assurance Certification and Accreditation Process (DIACAP), dated 28 Nov 2007 apply. This system is authorized for use to but not exceeding the Secret level only, and inappropriate or improper use of the system will result in a reportable incident to the Defense Security Service.

Applicable  Not Applicable.

**18. Receive Classified Documents.** *(8a and applies if 11b is marked yes)* Contract performance is restricted to: Contract facility listed in 8a and various government sites located in the National Capital Region; specified locations will be determine by the government contract monitor. AT&L will provide security classification guidance under performance of this contract. Contractor will receive classified documents only. Cleared personnel are required to perform this service because access to classified information cannot be precluded. The contractor is not authorized to release classified information to any activity or person, including sub-contractors, without the government Contracting Officer Representative's (COR) written approval. Only with the expressed permission of the government COR may the contractor reproduce any classified information/material. All requirements for control and accounting for original documentation and copies apply. All classified information must be marked in accordance with Executive Orders 12958 & 13292. All applicable provisions of DoD 5220.22M, National Industrial Security Program Operating Manual (NISPOM) and supplements apply.

Applicable  Not Applicable.

**19. Receive and Generate classified material.** *(Applies if block 11c is marked yes)* This contract requires the contractor to generate or perform work in support of creating classified documents. Classified information and materials shall be protected in accordance with the policies and procedures established by DoD Directive 5200.1-R, National Industrial Security Program Operating Instruction (NISPOM), dated January 1995, and all other applicable Executive Orders. Specific classification guidance will be provided on individual tasks by the COR or CM. The contractor must ensure that applicable classification guidance and marking provisions are complied with IAW the NISPOM. In any case where classification guidance has not been provided, the contractor is to safeguard the information and seek written guidance from the COR or CM prior to release of the information to anyone except the COR or CM.

Applicable  Not Applicable.

- a. The contractor must restrict access to only those individuals who possess the necessary security clearance and who are actually providing services under the contract with a valid need-to-know. Further dissemination to other contractors, subcontractors, other government agencies, private individuals or organizations is prohibited unless authorized in writing by the originating agency through the CM. Applies in all cases where paragraph 0 above is marked applicable.
- b. In cases where classified information is authorized to be stored or generated at the vendor facility, the contractor must ensure each employee having access to classified material is fully aware of the special security requirements for this material and shall maintain records in a manner that will permit the contractor to furnish, on demand, the names of individuals who have had access to this material in their custody. Applies in all cases where paragraph 19 above is marked applicable.
- c. Upon completion or termination of the classified contract, or sooner when the purpose of the release has been served, the contractor will return all classified information (furnished or generated) to the source from which received unless retention or other disposition instructions are authorized in writing by the COR. Applies in all cases where paragraph 19 above is marked applicable.
- d. The contractor must designate an individual who is working on the contract as custodian. The designated custodian shall be responsible for receipting and accounting for all classified material received under this contract. This does not mean that the custodian must personally sign for all classified material. The inner wrapper of all classified material dispatched should be marked for the attention of a designated custodian and must not be opened by anyone not working directly on the contract.

- e. Within 30 days after the final product is received and accepted by the procuring agency, classified intelligence materials released to or generated by the contractor, must be returned to the originating agency through the contract monitor unless written instructions authorizing destruction or retention are issued. Requests to retain material shall be directed to the CM for this contract in writing and must clearly indicate the justification for retention and identity of the specific document to be retained. Applies in all cases where paragraph 19 above is marked applicable.
- f. Classification, re-grading, or declassification markings of documentation produced by the contractor shall be consistent with that applied to the information or documentation from which the new document was prepared. If a compilation of information or a complete analysis of a subject appears to require a security classification other than that of the source documentation, the contractor shall assign the tentative security classification and request instructions from the contract monitor. Pending final determination, the material shall be safeguarded as required for its assigned or proposed classification, whichever is higher, until the classification is changed or otherwise verified. Applies in all cases where paragraph 19 above is marked applicable.

**20. Fabricate, Modify, or Store Classified Hardware.** *(Applies if 11d is marked yes)* Contracts will fabricate, modify, receive, and generate classified information and hardware. Contractor is authorized to process and store up to and incoming (Top Secret, Secret) information and hardware at contract facility listed in 6a. Actual knowledge and production of classified information is required for performance of this contract. Cleared personnel are required to perform this service because access to classified information cannot be precluded. The contractor is not authorized to release classified information to any activity or person, including sub-contractors, without the government Contracting Monitor's written approval. Only with the expressed permission of the government's Contracting Monitor may the contractor reproduce any classified information/material. All requirements for control and accounting for original documentation and copies apply.

Applicable  Not Applicable.

**21. Perform Services Only.** *(Mark block 11e yes and reference AT&L attachment 1 for specifics)* Actual knowledge and production of classified information is required for performance of this contract. Cleared personnel are required to perform this service because access to classified information cannot be precluded. The contractor is not authorized to release classified information to any activity or person, including sub-contractors, without the government Contracting Monitor's written approval. Only with the expressed permission of the government's Contracting Monitor may the contractor reproduce any classified information/material. All requirements for control and accounting for original documentation and copies apply. All applicable provisions for DoD 5220.22M and NISPOM supplements apply.

Applicable  Not Applicable.

**22. Have access to classified outside the U.S.** *(Applies if 11f is marked yes)* Contractor will require access to classified information outside the U.S. to include its possessions and Trusted Territories.

Applicable  Not Applicable.

**23. Government Travel.** *(Applies if 11f is marked yes)* As required by the Government Program Manager, contractors will be authorized travel/Temporary Duty (TDY) outside the NCR region for official government business. Note that if 11c is marked yes then 1b must have level of storage at contract facility. The government program Manager will provide travel orders and direction prior to departure.

Applicable  Not Applicable.

**24. DTIC Access Required.** *(Mark block 11g is marked yes)* Contractor is authorized to use the services of the Defense Technical Information Center (DTIC) and is required to prepare and process DD Form 1540. Contracting Officials, with concurrence from the program manager/project manager, must

Attachment 1 to the DD Form 254. DUSD (AT&L) Requirements for DoD Contractors

review and approve contractors need-to-know and ensure all identified DTIC information requirements are within Scope of Work prior to approving the DD Form 1540. Certification of need-to-know and use of DTIC field of interest register for the acquisition of reference materials classified through Top Secret/RD, disclosures authorizations, and visits clearance approvals, fall under the responsibility of the Contract Monitor (CM).

Applicable  Not Applicable.

**25. Require a COMSEC Account.** (Mark block 11h yes and reference AT&L attachment 1 for specifics)

Contractor must forward request for COMSEC material/information through government program manager to COMSEC monitor. Contractor is responsible for accountable COMSEC information and must provide a complete inventory as required by COMSEC account manager.

Applicable  Not Applicable.

**26. Emissions Security (AKA) TEMPEST.** (Applies if block 11i is marked yes) The contractor shall ensure that emissions security (EMSEC) conditions related to this contract are minimized.

Applicable  Not Applicable.

**27. Operations Security.** (Applies if block 11j is marked yes) The contractor shall comply with OPSEC requirements specified in DoD 5220-22-M, National Industrial Security Program Operating Manual (NISPOM). OPSEC requirements are applicable to the contractor's SAP procedures but only if specified by the SAP Program Office.

Applicable  Not Applicable.

**28. Authorized to use Defense Courier Service.** (Applies if 11k is marked yes) Contractor must obtain written approval from the contracting activity and provide the request for DCS services to Commander, Defense Courier Service, Attn: Operations Division, Fort George G. Meade, MD. 20755-5370. Prior approval of the contracting activity is required before granting subcontractor use of DCS services.

Applicable  Not Applicable.

**29. Courier authorizations.** (Mark block 11l yes and reference AT&L attachment 1 for specifics) This contract requires personnel to obtain the Government issued Courier Authorization. All courier authorizations will be in accordance with the NISPOM. As such, all contractor personnel are required to in-process with the Administration Directorate Security Office to obtain courier cards. Instructions for obtaining the courier card is contained on the AT&L intranet home page and must be adhered to in order to obtain the courier card. As a condition of this contract, all personnel issued Courier Cards are required to ensure the card is returned to the AT&L Security Office or the CAC Coordinator upon removal from the contract or termination of employment under this contract.

Applicable  Not Applicable.

**30. Performance as Office Security Managers.** (Mark block 11l yes and reference AT&L attachment 1 for specifics) Contractor may require performance as alternate Office Security Manager.

Responsibilities of the Office Security Manager are contained on the AT&L intranet home page and must be adhered to.

Applicable  Not Applicable.

**31. Performance as Activity Security Reprehensive.** (Mark block 11l yes and reference AT&L attachment 1 for specifics) Contractor may require performance as alternate Terminal Area Security

Attachment 1 to the DD Form 254. DUSD (AT&L) Requirements for DoD Contractors

Officer. Responsibilities of the Terminal Area Security Officer are contained on the AT&L intranet home page and must be adhered to.

Applicable                       Not Applicable.

**32.IT Operation and Support Positions.** (Mark block 111 yes and reference AT&L attachment 1 for specifics) Contract will require access to sensitive unclassified government automated information systems (AIS) at different levels. Contractor must comply with the attached WHS IT Policy Bulletin 2004-0003.

Applicable                       Not Applicable.

**COORDINATION:**

Contracting Officer's Representative \_\_\_\_\_ Date \_\_\_\_\_

AT&L Security Office \_\_\_\_\_ Date \_\_\_\_\_

PFPA Industrial Security \_\_\_\_\_ Date \_\_\_\_\_

PFPA COMSEC Office \_\_\_\_\_ Date \_\_\_\_\_

SAP Program Manager \_\_\_\_\_ N/A \_\_\_\_\_ Date \_\_\_\_\_  
(if applicable)

Restricted Data Manager \_\_\_\_\_ N/A \_\_\_\_\_ Date \_\_\_\_\_  
(if applicable)

NATO Program Manager \_\_\_\_\_ N/A \_\_\_\_\_ Date \_\_\_\_\_  
(if applicable)

### Attachment 2 to the DD Form 254. FOUO Requirements for DoD Contractors

---

The following procedures will be used to protect FOR OFFICIAL USE ONLY (FOUO) materials:

1. **HANDLING:** Access to FOUO material shall be limited to those employees needing the material to perform their duties. The FOUO marking is assigned to material created by a DoD User Agency. FOUO is not a classification, but requires extra precautions to ensure it is not released to the public.
2. **MARKING:** Mark unclassified documents containing FOUO: “FOR OFFICIAL USE ONLY at the bottom of each page and back cover (if any). In a classified document:
  - a. Mark individual paragraph that contains FOUO, but not classified material by placing “FOUO at the beginning of the paragraph.
  - b. Mark top and bottom of each page that has both FOUO and classified material with the highest security classification of the material on that page.
  - c. Mark “FOUO at the bottom of each page that has FOUO but not classified material.
  - d. If a classified document also contains FOUO material or if the classified material becomes FOUO when declassified, place the following statement on the bottom of the cover or the first page under the classification marking: “NOTE: If declassified, review the document to make sure the material is not FOUO and not exempt under DoD Regulation 5400.7 before public release.
  - e. Mark other records such as computer print outs, photographs, films, tapes,, Or slides FOR OFFICIAL USE ONLY” so the receiver or viewer knows the record contains FOUO material.
  - f. Mark each part of a message that contains FOUO material. Unclassified messages containing FOUO material must show the abbreviation “FOUO before the text begins.
  - g. Ensure documents that transmit FOUO material call attention to any FOUO attachments.
  - h. FOUO material released to a contractor by a DoD user agency must have the following statement on the front page or cover: 11-118 DOCUMENT CONTAINS MATERIAL EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT. EXEMPTION(S)\_\_\_\_\_APPLY.”
3. **STORAGE:** During normal duty hours, place FOUO material in an out-of-sight location if your work area is accessible to persons who do not have a valid need for the material. After normal duty hours, store FOUO material to prevent unauthorized access. File with other unclassified records in unlocked files or desks when internal building security is provided. When there is no internal security, locked buildings or rooms usually provide adequate after hours protection. For additional protection, store FOUO material in locked containers such as file cabinets, desks, or bookcases. Expenditure of funds for security containers or closed areas solely for the protection of FOUO material is prohibited –
4. **TRANSMISSION:** FOUO documents and materials may be transmitted via first class mail, parcel post or for bulky shipments-fourth class mail. Within the CONUS discussion of FOUO material on the telephone is authorized if necessary for the performance of the contract. Electronic transmission of FOUO information (voice, data or facsimile) should be by approved secure communications systems whenever practical.
5. **RELEASE:** FOUO material shall not be released outside of the contractor’s facility except to the representative of the DOD.
6. **DESTRUCTION:** When no longer needed FOUO material shall be disposed of by a method that precludes its disclosure to unauthorized individuals.



**Release of Non-SCI Intelligence Information to DoD Contractors**

ATTACHMENT TO DD FORM 254 FOR CONTRACT NO:  
CONTRACT EXPIRATION DATE:

1. Requirements for access to non-SCI:

- a. All intelligence material released to the contractor remains the property of the US Government and may be withdrawn at any time. Contractors must maintain accountability for all classified intelligence released into their custody.
- b. The contractor must not reproduce intelligence material without the written permission of the originating agency through the Intelligence Support Office. If permission is granted, each copy shall be controlled in the same manner as the original.
- c. The contractor must not destroy any intelligence material without advance approval or as specified by the contract monitor (CM). (EXCEPTION: Classified waste shall be destroyed as soon as practicable in accordance with the provisions of the Industrial Security Program).
- d. The contractor must restrict access to only those individuals who possess the necessary security clearance and who are actually providing services under the contract with a valid need-to-know. Further dissemination to other contractors, subcontractors, other government agencies, private individuals or organizations is prohibited unless authorized in writing by the originating agency through the CM.
- e. The contractor must ensure each employee having access to intelligence material is fully aware of the special security requirements for this material and shall maintain records in a manner that will permit the contractor to furnish, on demand, the names of individuals who have had access to this material in their custody.
- f. Intelligence material must not be released to foreign nationals or immigrant aliens whether they are consultants, US contractors, or employees of the contractor and regardless of the level of their security clearance, except with advance written permission from the originator. Requests for release to foreign nationals shall be initially forwarded to the contract monitor and shall include:
  - (1) A copy of the proposed disclosure.
  - (2) Full justification reflecting the benefits to US interests.
  - (3) Name, nationality, particulars of clearance, and current access authorization of each proposed foreign national recipient.
- g. Upon completion or termination of the classified contract, or sooner when the purpose of the release has been served, the contractor will return all classified intelligence (furnished or generated) to the source from which received unless retention or other disposition instructions (see DCID 6/1 ) are authorized in writing by the CM.
- h. The contractor must designate an individual who is working on the contract as custodian. The designated custodian shall be responsible for receipting and accounting for all classified intelligence material received under this contract. This does not mean that the custodian must personally sign for all classified material. The inner wrapper of all classified material dispatched should be marked for the attention of a designated custodian and must not be opened by anyone not working directly on the contract.
- i. Within 30 days after the final product is received and accepted by the procuring agency, classified intelligence materials released to or generated by the contractor, must be returned to the originating agency through the contract monitor unless written instructions authorizing destruction or retention are issued. Requests to retain material shall be directed to the CM for this contract in writing and must clearly indicate the justification for retention and identity of the specific document to be retained.

## Attachment 3 to the DD Form 254. Non-SCI Requirements for DoD Contractors

- j. Classification, re-grading, or declassification markings of documentation produced by the contractor shall be consistent with that applied to the information or documentation from which the new document was prepared. If a compilation of information or a complete analysis of a subject appears to require a security classification other than that of the source documentation, the contractor shall assign the tentative security classification and request instructions from the contract monitor. Pending final determination, the material shall be safeguarded as required for its assigned or proposed classification, whichever is higher, until the classification is changed or otherwise verified.
2. Intelligence material carries special markings. The following is a list of the authorized control markings of intelligence material:
    - a. “Dissemination and Extraction of Information Controlled by Originator (ORCON).” This marking is used, with a security classification, to enable a continuing knowledge and supervision by the originator of the use made of the information involved. This marking may be used on intelligence which clearly identifies, or would reasonably permit ready identification of an intelligence source or method, which is particularly susceptible to countermeasures that would nullify or measurably reduce its effectiveness. This marking may not be used when an item or information will reasonably be protected by use of other markings specified herein, or by the application of the “need-to-know” principle and the safeguarding procedures of the security classification system.
    - b. “Authorized for Release to (Name of Country(ies)/International Organization.” The above is abbreviated “REL \_\_\_\_\_.” This marking must be used when it is necessary to identify classified intelligence material the US government originator has predetermined to be releasable or has been released through established foreign disclosure channels to the indicated country(ies) or organization.
  3. The following procedures govern the use of control markings.
    - a. Any recipient desiring to use intelligence in a manner contrary to restrictions established by the control marking set forth above shall obtain the advance permission of the originating agency through the CM. Such permission applies only to the specific purposes agreed to by the originator and does not automatically apply to all recipients. Originators shall ensure that prompt consideration is given to recipients’ requests in these regards, with particular attention to reviewing and editing, if necessary, sanitized or paraphrased versions to derive a text suitable for release subject to lesser or no control markings.
    - b. The control marking authorized above shall be shown on the title page, front cover, and other applicable pages of documents, incorporated in the text of electrical communications, shown on graphics, and associated (in full or abbreviated form) with data stored or processed in automatic data processing systems. The control marking also shall be indicated by parenthetical use of the marking abbreviations at the beginning or end of the appropriate portions. If the control marking applies to several or all portions, the document must be marked with a statement to this effect rather than marking each portion individually.
    - c. The control markings shall be individually assigned at the time of preparation of intelligence products and used in conjunction with security classifications and other marking specified by E.O. 12958 and its implementing security directives. The marking shall be carried forward to any new format in which the same information is incorporated including oral and visual presentations.
  4. Request for release of intelligence material to a contractor must be prepared by the contract monitor (CM) and submitted to the Intelligence Support Office. This should be accomplished as soon as possible after the contract has been awarded. The request will be prepared and accompanied with a letter explaining the requirements and copies of the DD Form 254 and Statement of Work.

**RELEASE OF SENSITIVE COMPARTMENTED INFORMATION (SCI)  
INTELLIGENCE INFORMATION TO US CONTRACTORS**

ATTACHMENT TO DD FORM 254 FOR CONTRACT NO:

SCI BILLETS AUTHORIZED:

CONTRACT EXPIRATION DATE:

1. Requirements for access to SCI:

- a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).
- b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.
- c. Names of contractor personnel requiring access to SCI will be submitted to the contract monitor (CM) for approval. (The contract monitor is identified on the reverse side of the DD Form 254.) Upon receipt of written approval from the CM, the company security officer will submit request(s) for special background investigations in accordance with the NISPOM, to the Intelligence Support Office. The entire personnel security questionnaire package should not be forwarded to the Intelligence Support Office. The Contractor Special Security Officer (CSSO) must follow the instructions provided by the Intelligence Support Office to the CSSO.
- d. Inquiries pertaining to classification guidance on SCI will be directed through the CSSO to the responsible CM as indicated on the DD Form 254.
- e. SCI furnished in support of this contract remains the property of the Department of Defense (DoD) department, agency, or command originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the CM.
- f. SCI will be stored and maintained only in properly accredited facilities at the contractor location.

2. The contract monitor (CM) will:

- a. Review the SCI product for contract applicability and determine that the product is required by the contractor to complete contractual obligations. After the CM has reviewed the SCI product(s) for contract applicability and determined that the product is required by the contractor to complete obligations, the CM must request release from the originator through the Intelligence Division. Originator release authority is required on the product types below:
  - (1) Documents bearing the control markings of ORCON, PROPIN.
  - (2) GAMMA controlled documents.
  - (3) Any NSA/SPECIAL marked product.
  - (4) All categories as listed in DoD 5105.21-M-1
- b. Prepare or review contractor billet/access requests to insure satisfactory justification (need-to-know) and completeness of required information.
- c. Approve and coordinate visits by contractor employees when such visits are conducted as part of the contract effort.

## Attachment 3 to the DD Form 254. Non-SCI Requirements for DoD Contractors

- d. Maintain records of all SCI material provided to the contractor in support of the contract effort. By 15 January (annually), provide the contractor, for inventory purposes, with a complete list of all documents transferred by contract number, organizational control number, copy number, and document title.
- e. Determine dissemination of SCI studies or materials originated or developed by the contractor.
- f. Within 30 days after completion of the contract, provide written disposition instructions for all SCI material furnished to, or generated by, the contractor with an information copy to the supporting SSO.
- g. Review and forward all contractor requests to process SCI electronically to the accrediting SSO for coordination through appropriate SCI channels.
- h. Request for release of intelligence material to a contractor must be prepared by the contract monitor (CM) and submitted to the Intelligence Support Office. This should be accomplished as soon as possible after the contract has been awarded. The request will be prepared and accompanied with a letter explaining the requirement and copies of the DD Form 254 and Statement of Work.

The following procedures will be used to protect Proprietary & Sensitive But Unclassified materials and information within AT&L:

1. **HANDLING:** Access to Proprietary & Sensitive But Unclassified materials and information within AT&L material shall be done in the same manner as that of FOUO information. Access to the information is limited to those employees needing the material to perform their duties. Proprietary information is the property of the individual company which provided the information and remains the property of that company, entrusted to the DoD. It is incumbent upon the DoD to ensure that unauthorized or unintended dissemination is prevented. Proprietary is not a classification, but requires extra precautions to ensure it is not released to the public.
2. **MARKING:** Mark Proprietary documents containing “Proprietary” at the bottom of each page and back cover (if any). In a classified document:
  - a. Mark individual paragraph that contains Proprietary, but not classified material by placing “Proprietary” at the beginning of the paragraph.
  - b. Mark top and bottom of each page that has both Proprietary and classified material with the highest security classification of the material on that page.
  - c. Mark “Proprietary” at the bottom of each page that has Proprietary but not classified material.
  - d. If a classified document also contains Proprietary material or is the classified material becomes Proprietary when declassified, place the following statement on the bottom of the cover or the first page under the classification marking: “NOTE: If declassified, review the document to make sure the material is not Proprietary and not exempt under DoD Regulation 5400.7 before public release.
  - e. Mark other records such as computer print outs, photographs, films, tapes, Or slides “Proprietary” so the receiver or viewer knows the record contains Proprietary material.
  - f. Mark each part of a message that contains Proprietary material.
  - g. Ensure documents that transmit Proprietary material call attention to any Proprietary attachments.
  - h. Proprietary material released to a contractor by a DoD user agency must have the following statement on the front page or cover: 11-118 DOCUMENT CONTAINS MATERIAL EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT. EXEMPTION(S)\_\_\_\_\_APPLY.”
3. **STORAGE:** During normal duty hours, place Proprietary material in an out-of-sight location if your work area is accessible to persons who do not have a valid need for the material. After normal duty hours, store

Proprietary material to prevent unauthorized access. File with other unclassified records in unlocked files or desks when internal building security is provided. When there is no internal security, locked buildings or rooms usually provide adequate after hours protection. For additional protection, store Proprietary material in locked containers such as file cabinets, desks, or bookcases. Expenditure of funds for security containers or closed areas solely for the protection of Proprietary material is prohibited.

4. **TRANSMISSION:** Proprietary documents and materials may be transmitted via first class mail, parcel post or for bulky shipments-fourth class mail. Within the CONUS discussion of Proprietary material on the telephone is authorized if necessary for the performance of the contract. Electronic transmission of Proprietary information (voice, data or facsimile) should be by approved secure communications systems whenever practical.
5. **RELEASE.** Proprietary material shall not be released outside of the contractor's facility except to the representative of the DOD.
6. **DESTRUCTION:** When no longer needed Proprietary material shall be disposed of by a method that precludes its disclosure to unauthorized individuals.