



DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

OFFICE OF THE SECRETARY

DoDM5200.01V1_DAFMAN_16-1404V1_DAFGM2025-01

28 August 2025

MEMORANDUM FOR ALMAJCOM-ALFLDCOM-FOA-DRU/CC
DISTRIBUTION C

FROM: SAF/OC
1720 Air Force Pentagon
Washington DC 20330-1720

SUBJECT: Department of the Air Force Guidance Memorandum to
DoDM5200.01V1_DAFMAN_16-1404V1, *DoD Information Security Program:
Overview, Classification, and Declassification*

By Order of the Secretary of the Air Force, this Guidance Memorandum (GM) immediately reissues the current August 2024 GM to DoDM5200.01V1_DAFMAN16-1404V1, establishing requirements for conducting quarterly random entry/exit inspections of vaults and open storage areas/rooms processing or storing high volumes of classified information, as determined by the Installation Commander. This memorandum does not supersede or eliminate requirements to conduct end-of-day checks of areas or rooms containing approved security containers. Compliance with this memorandum is mandatory. To the extent its directions are inconsistent with other Department of the Air Force publications, the information herein prevails, in accordance with DAFI 90-160, *Publications and Forms Management*.

This memorandum becomes void after one year has elapsed from the date of this memorandum or upon publishing of DoDM5200.01V1_DAFMAN16-1404V1 permanently establishing this guidance, whichever is earlier.

EDWIN H. OSHIBA, SES, DAF
Director, Competitive Activities

Guidance Changes

7n(5) **(Added)(DAF)** The Wing/Delta (Installation) Commander will:

(j) Establish and implement procedures for random entry/exit inspections of vaults and open storage areas/rooms, processing or significant amounts of classified information, at least quarterly. These inspections are designed to prevent the unauthorized introduction of prohibited devices and validate authorization of the removal of classified information/material from vaults and open storage areas/rooms. The servicing Staff Judge Advocate (SJA) must complete a review of these procedures.

(1) **(Added)(DAF)** Establish a random entry/exit inspection schedule of vaults and open storage areas/rooms, processing or storing significant amounts of classified information. The inspection schedule should cover the duration of inspection (e.g., 1 hour or 3 hours), the frequency of inspection (e.g., every 3 persons or every 5 persons) and the method of inspection. (e.g., pockets, wrists, and bags of all persons, visual inspection only) It is recommended that the Installation Commander appoint members of each gender to conduct entry/exit inspections and mandate visual-only inspections of personnel. Inspectors should provide the results to the Wing/Delta installation information protection (IP) office and contact SJA if they believe further personnel inspection is required.

Note: A determination of what constitutes significant amounts of classified processing or storage is left to the Commander's discretion.

- (2) **(Added)(DAF)** Ensure inspection procedures are codified in writing and available for review where the inspections are being conducted.
- (3) **(Added)(DAF)** Ensure inspection procedures include specific actions the inspection official must take if an unapproved item/device is identified and/or if they suspect a security incident such as someone attempting to remove information without approval. This includes having the inspection immediately stopped in order to report the matter to the cognizant investigative authority (See Enclosure 6 of Volume 3).
- (4) **(Added)(DAF)** Ensure personnel tasked with performing these inspections are trained IAW approved procedures.
- (5) **(Added)(DAF)** Document and maintain an accountability log of each check. At a minimum, and as per servicing SJA coordination, maintain documentation indicating when (date/time) the checks were completed, the total number of personnel inspected, and the results of the inspection, if contraband/prohibited items were discovered.



DEPARTMENT OF THE AIR FORCE MANUAL
16-1404, Volume 1

6 APRIL 2022

Operations Support

**INFORMATION SECURITY PROGRAM:
OVERVIEW, CLASSIFICATION, AND DECLASSIFICATION**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing web site, at www.ePublishing.af.mil.

RELEASABILITY: There are no release restrictions on this publication.

OPR: SAF/AAZO

Certified by: SAF/AAZ
(Ms. Jennifer M. Aquinas, SES, DAF)

Supersedes: DoDM 5200.01V1_AFMAN 16-1404V1, 11 January 2021

Pages: 111

This publication implements guidance in Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance* (reference (bt)). The Department of Defense Manual (DoDM) 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*, is printed, word-for-word in regular font, without change. Department of the Air Force (DAF) supplemental material is printed in bold font and indicated by “(Added)(DAF)” for changes and additions, from the last iteration. It describes DAF responsibilities and establishes the requirements to support the Department of Defense (DoD) information security program.

This guidance applies to all civilian employees, uniformed members of the Regular Air Force, the Air Force Reserve, the Air National Guard, the Civil Air Patrol (when conducting missions as the official Air Force Auxiliary), the United States Space Force (USSF), and contractor support personnel when stated in the contract or DD Form 254, *Department of Defense Contract Security Classification Specification*, except where noted otherwise.

Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFI 33-322, *Records Management and Information Governance Program* (reference (bq)), and disposed of in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System.

Refer recommended changes and questions to the office of primary responsibility (OPR) listed above, using the AF Form 847, *Recommendation for Change of Publication*, and route through the local information protection office. This publication may be supplemented at any level, but all supplements will be routed to the OPR prior to certification and approval.

The authorities to waive wing/Space Force equivalent/unit level requirements in this publication are identified with a Tier (“T-0, T-1, T-2, T-3”) number following the compliance statement. See DAFI 33-360, *Publications and Forms Management* (reference (bp)), for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor’s commander for non-tiered compliance items.

The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the DAF.

Compliance with the appendix to enclosure 6, in this publication, is mandatory.

As used throughout this Manual, the term “MAJCOM” (Major Command) includes a direct reporting unit and a field operating agency. The term “FLDCOM” (Field Command) represents Space Force organizations. The term “wing” includes “delta,” and “garrison,” for Space Force organizational responsibilities.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Key changes include, changing the requirement to establish a top secret accountability system (i.e., registry); the requirement to conduct an 100% top secret annual inventory is now at commander/director’s discretion vice mandatory (see enclosure 3, section 6); and, updates to the security classification guide (SCG) requirements in enclosure 6. An asterisk (*) indicates newly revised material.



Department of Defense MANUAL

NUMBER 5200.01, Volume 1
February 24, 2012
Incorporating Change 2, July 28, 2020

USD(I&S)

SUBJECT: DoD Information Security Program: Overview, Classification and Declassification

References: See Enclosure 1

1. PURPOSE

a. Manual. This Manual is composed of several volumes, each containing its own purpose. The purpose of the overall Manual, as authorized by DoD Directive (DoDD) 5143.01 (Reference (a)) and DoD Instruction (DoDI) 5200.01 (Reference (b)), is to reissue DoD 5200.1-R (Reference (c)) as a DoD Manual (DoDM) to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI) and Special Access Program (SAP). This guidance is developed in accordance with Reference (b), Executive Order (E.O.) 13526 and E.O. 13556, and parts 2001 and 2002 of title 32, Code of Federal Regulations (References (d), (e), and (f)). This combined guidance is known as the DoD Information Security Program.

b. Volume. This Volume:

- (1) Describes the DoD Information Security Program.
- (2) Provides guidance for classification and declassification of DoD information that requires protection in the interest of the National Security.
- (3) Cancels Reference (c) and DoD O-5200.1-I (Reference (g)).
- (4) Incorporates and cancels Directive-Type Memorandums 04-010 (Reference (h)) and 11-004 (Reference (i)).

c. (Added)(DAF) This Department of the Air Force Manual (DAFMAN) is composed of three volumes, each containing its own purpose.

(1) (Added)(DAF) SCI shall be safeguarded in accordance with paragraph 2.b., below. (T-0).

(2) (Added)(DAF) SAP shall be safeguarded in accordance with DoDI 5205.11, *Management, Administration, and Oversight of DoD Special Access Programs (SAPs)*, AFI 16-701, *Management, Administration and Oversight of Special Access Programs* (reference (br)), and other applicable guidance. (T-0).

2. APPLICABILITY. This Volume:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the “DoD Components”).

b. It does not alter existing authorities and responsibilities of the Director of National Intelligence (DNI) or of the heads of elements of the Intelligence Community pursuant to policies issued by the DNI. Consistent with Reference (b), SCI shall be safeguarded in accordance with the policies and procedures issued by the DNI, as implemented by DoDM 5105.21 (Reference (j)), and other applicable guidance.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy, in accordance with Reference (b), to:

a. Identify and protect national security information and CUI in accordance with national level policy issuances.

b. Promote information sharing, facilitate judicious use of resources, and simplify management through implementation of uniform and standardized processes.

c. Classify and declassify national security information as required by References (d) and (f).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosures 3 through 6.

7. INFORMATION COLLECTION REQUIREMENTS

a. The Annual Report on Classified Information referenced in paragraph 7.m. of Enclosure 2 of this Volume has been assigned Report Control Symbol (RCS) DD-INT(AR)1418 in accordance with the procedures in Volume 1 of DoDM 8910.01 (Reference (k)).

b. The DoD Security Classification Guide Data Elements, DD Form 2024, “DoD Security Classification Guide Certified Data Elements,” referenced in section 6 of Enclosure 6 of this Volume, has been assigned RCS DD-INT(AR)1418, in accordance with the procedures in Reference (k).

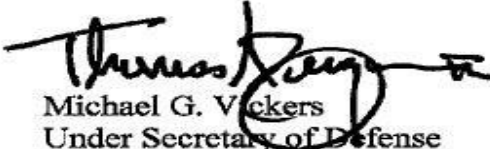
8. RELEASABILITY. *Cleared for public release*. This Volume is available on the DoD Issuances Website at <https://www.esd.whs.mil/DD>.

9. SUMMARY OF CHANGE 2. This administrative change updates:

a. The title of the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Intelligence and Security (USD(I&S)) in accordance with Public Law 116-92 (Reference (bo)).

b. Administrative changes in accordance with current standards of the Office of the Chief Management Officer of the DoD.

10. EFFECTIVE DATE. This Volume is effective February 24, 2012.



Michael G. Vickers
Under Secretary of Defense
for Intelligence

ANTHONY P. REARDON, SES, DAF
Administrative Assistant

Enclosures

1. References
2. Responsibilities
3. DoD Information Security Program Overview
4. Classifying Information
5. Declassification and Changes in Classification
6. Security Classification Guides

Glossary

TABLE OF CONTENTS

1		
2		
3		
4		
5	ENCLOSURE 1: REFERENCES.....	10
6		
7	ENCLOSURE 2: RESPONSIBILITIES.....	14
8		
9	USD(I&S).....	14
10	UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)).....	15
11	DoD CHIEF INFORMATION OFFICER (CIO).....	15
12	ADMINISTRATOR, DEFENSE TECHNICAL INFORMATION CENTER (DTIC).....	16
13	DIRECTOR, WHITE HOUSE STAFF (WHS).....	16
14	HEADS OF THE DoD COMPONENTS.....	16
15	SENIOR AGENCY OFFICIALS.....	17
16	*(Added)(DAF) DAF Information Security Program.....	21
17	HEADS OF DoD ACTIVITIES.....	27
18	ACTIVITY SECURITY MANAGER.....	28
19	TOP SECRET CONTROL OFFICER (TSCO).....	30
20	SENIOR INTELLIGENCE OFFICIALS.....	30
21	INFORMATION SYSTEMS SECURITY OFFICIALS.....	31
22		
23	ENCLOSURE 3: DoD INFORMATION SECURITY PROGRAM OVERVIEW.....	32
24		
25	PURPOSE.....	32
26	SCOPE.....	32
27	PERSONAL RESPONSIBILITY.....	32
28	NATIONAL AUTHORITIES FOR SECURITY MATTERS.....	32
29	President of the United States.....	32
30	National Security Council (NSC).....	32
31	DNI.....	33
32	Information Security Oversight Office (ISOO).....	33
33	CUI Office (CUIO).....	33
34	DoD INFORMATION SECURITY PROGRAM MANAGEMENT.....	33
35	USD(I&S).....	33
36	USD(P).....	33
37	DoD CIO.....	34
38	National Security Agency/Central Security Service (NSA/CSS).....	34
39	DIA.....	34
40	Defense Counterintelligence and Security Agency (DCSA).....	34
41	DTIC.....	34
42	DoD COMPONENT INFORMATION SECURITY MANAGEMENT.....	34
43	Head of the DoD Component.....	34
44	Senior Agency Officials.....	35
45	Activity Security Management.....	35
46	TSCO.....	36
47	Other Security Management Roles.....	37
48		

49	USE OF CONTRACTORS IN SECURITY ADMINISTRATION.....	38
50	USE OF FOREIGN NATIONALS IN SECURITY ADMINISTRATION.....	39
51	CLASSIFICATION AUTHORITY.....	40
52	CLASSIFICATION POLICY.....	40
53	RECLASSIFICATION.....	40
54	ACCESS TO CLASSIFIED INFORMATION.....	40
55	Requirements for Access.....	40
56	Nondisclosure Agreements	40
57	NATO Briefing for Cleared Personnel.....	41
58	Access by Individuals outside the Executive Branch.....	41
59	PROTECTION REQUIREMENTS.....	41
60	Protection of Restricted Data (RD) and Formerly Restricted Data (FRD).....	41
61	Protection of SCI.....	42
62	Protection of COMSEC Information.....	42
63	Protection of SAP Information.....	42
64	Protection of NATO and FGI.....	42
65	Protection of Nuclear Command and Control-Extremely Sensitive Information (NC2-	
66	ESI).....	42
67	RETENTION	43
68	PERMANENTLY VALUABLE RECORDS.....	43
69	MILITARY OPERATIONS	43
70	WAIVERS AND EXCEPTIONS.....	43
71	CORRECTIVE ACTIONS AND SANCTIONS.....	44
72	Procedures.....	44
73	Sanctions.....	44
74	Reporting of Incidents.....	45
75	APPENDIX: DoD COMPONENT REQUEST FOR WAIVER OR EXCEPTION.....	46
76		
77	ENCLOSURE 4: CLASSIFYING INFORMATION.....	47
78		
79	CLASSIFICATION POLICY.....	47
80	CLASSIFICATION PROHIBITIONS.....	48
81	LEVELS OF CLASSIFICATION.....	48
82	Top Secret	48
83	Secret.....	48
84	Confidential.....	48
85	ORIGINAL CLASSIFICATION.....	48
86	REQUESTS FOR OCA.....	47
87	ORIGINAL CLASSIFICATION PROCESS.....	51
88	CHANGING THE LEVEL OF CLASSIFICATION.....	52
89	SECURITY CLASSIFICATION GUIDANCE.....	52
90	TENTATIVE CLASSIFICATION.....	53
91	DERIVATIVE CLASSIFICATION.....	53
92	RESPONSIBILITIES OF DERIVATIVE CLASSIFIERS	53
93	PROCEDURES FOR DERIVATIVE CLASSIFICATION.....	54
94	DURATION OF CLASSIFICATION.....	55
95	Originally Classified Information.....	55
96	Derivatively Classified Information.....	55
97	Extending the Duration of Classification.....	55
98	FORMAT FOR DISSEMINATION.....	56

99	COMPILATIONS.....	56
100	CLASSIFICATION OF ACQUISITION INFORMATION.....	57
101	CLASSIFICATION OF INFORMATION RELEASED TO THE PUBLIC.....	57
102	Classified Information Released Without Proper Authority.....	58
103	Reclassification of Information Declassified and Released to the Public under Proper	
104	Authority.....	58
105	Information Declassified and Released to the Public without Proper Authority.....	60
106	CLASSIFICATION OR RECLASSIFICATION FOLLOWING RECEIPT OF A REQUEST	
107	FOR INFORMATION.....	60
108	CLASSIFYING NON-GOVERNMENT RESEARCH AND DEVELOPMENT	
109	INFORMATION.....	61
110	THE PATENT SECRECY ACT OF 1952.....	61
111	REQUESTS FOR CLASSIFICATION DETERMINATION.....	62
112	CHALLENGES TO CLASSIFICATION.....	62
113	Principles.....	62
114	Procedures.....	63
115		
116	ENCLOSURE 5: DECLASSIFICATION AND CHANGES IN CLASSIFICATION.....	65
117		
118	DECLASSIFICATION POLICY.....	65
119	PROCESSES FOR DECLASSIFICATION.....	66
120	AUTHORITY TO DECLASSIFY.....	66
121	DECLASSIFICATION GUIDANCE.....	68
122	DECLASSIFICATION OF INFORMATION.....	68
123	CANCELING OR CHANGING CLASSIFICATION MARKINGS.....	68
124	SPECIAL PROCEDURES FOR CRYPTOLOGIC INFORMATION.....	69
125	PERMANENTLY VALUABLE RECORDS.....	69
126	RECORDS DETERMINED NOT TO HAVE PERMANENT HISTORICAL VALUE.....	69
127	EXTENDING CLASSIFICATION BEYOND 25 YEARS FOR UNSCHEDULED	
128	RECORDS.....	70
129	CLASSIFIED INFORMATION IN THE CUSTODY OF CONTRACTORS, LICENSEES,	
130	GRANTEES, OR OTHER AUTHORIZED PRIVATE ORGANIZATIONS OR	
131	INDIVIDUALS.....	70
132	AUTOMATIC DECLASSIFICATION.....	70
133	Deadline.....	70
134	Secretary of Defense Certification.....	70
135	Public Release of Automatically Declassified Documents.....	71
136	Basis for Exclusion or Exemption from Automatic Declassification.....	71
137	Exclusion of RD and FRD.....	71
138	Integral File Block.....	71
139	Delays of Automatic Declassification.....	72
140	Automatic Declassification of Backlogged Records at NARA.....	73
141	Declassification Review Techniques.....	73
142	EXEMPTIONS FROM AUTOMATIC DECLASSIFICATION.....	73
143	Exemption Types.....	74
144	Exemption Criteria and Duration.....	74
145	Exemption Requests.....	75
146	When to Request an Exemption.....	77
147	Who Identifies and Requests an Exemption.....	77
148	ISCAP Authority.....	77

149	Notice to Information Holders	77
150	DECLASSIFICATION OF INFORMATION MARKED WITH OLD DECLASSIFICATION	
151	INSTRUCTIONS.....	77
152	REFERRALS IN THE AUTOMATIC DECLASSIFICATION PROCESS.....	78
153	Description.....	78
154	Referral Responsibility	78
155	MANDATORY DECLASSIFICATION REVIEW	78
156	SYSTEMATIC REVIEW FOR DECLASSIFICATION	82
157	DOWNGRADING CLASSIFIED INFORMATION	82
158	UPGRADING CLASSIFIED INFORMATION	83
159	DECLASSIFYING FGI.....	83
160	APPLICATION OF DECLASSIFICATION AND EXTENSION OF CLASSIFICATION TO	
161	PRESENT AND PREDECESSOR EXECUTIVE ORDERS.....	84
162		
163	ENCLOSURE 6: SECURITY CLASSIFICATION GUIDES	85
164		
165	GENERAL.....	85
166	CONTENT OF SECURITY CLASSIFICATION GUIDES.....	85
167	CUI AND UNCLASSIFIED ELEMENTS OF INFORMATION.....	86
168	DATA COMPILATION CONSIDERATIONS	86
169	APPROVAL OF SECURITY CLASSIFICATION GUIDES.....	87
170	DISTRIBUTION OF SECURITY CLASSIFICATION GUIDES.....	87
171	INDEX OF SECURITY CLASSIFICATION GUIDES.....	88
172	REVIEW OF SECURITY CLASSIFICATION GUIDES.....	88
173	REVISION OF SECURITY CLASSIFICATION GUIDES.....	88
174	CANCELLING SECURITY CLASSIFICATION GUIDES.....	88
175	REPORTING CHANGES TO SECURITY CLASSIFICATION GUIDES.....	89
176	FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEWS	89
177	*(Added)(DAF) APPENDIX: SECURITY CLASSIFICATION GUIDE FORMAT.....	90
178		
179	GLOSSARY.....	101
180	PART I. ABBREVIATIONS AND ACRONYMS.....	101
181	PART I.A. *(Added)(DAF) ACRONYMS.....	102
182	PART II. DEFINITIONS.....	103
183		
184		

...

ENCLOSURE 1REFERENCES

- 185
186
187
188
189
190 (a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I&S))," October
191 24, 2014, as amended
192 (b) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive
193 Compartmented Information (SCI)," April 21, 2016
194 (c) DoD 5200.1-R, "Information Security Program," January 14, 1997 (hereby cancelled)
195 (d) Executive Order 13526, "Classified National Security Information," December 29, 2009
196 (e) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010
197 (f) Parts 2001 and 2002 of title 32, Code of Federal Regulations
198 (g) DoD O-5200.1-I, "Index of Security Classification Guides," September 1, 1996 (hereby
199 cancelled)
200 (h) Directive-Type Memorandum 04-010, "Interim Information Security Guidance," April 16,
201 2004 (hereby cancelled)
202 (i) Directive-Type Memorandum 11-004, "Immediate Implementation Provisions of Executive
203 Order (hereby cancelled)
204 (j) DoD Manual 5105.21, Volumes 1-3, "Sensitive Compartmented Information (SCI)
205 Administrative Security Manual," October 19, 2012
206 (k) DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD
207 Internal Information Collections," June 30, 2014, as amended
208 (l) Section 2723 of title 10, United States Code
209 (m) DoD Directive 5210.50, "Management of Serious Security Incidents Involving Classified
210 Information," October 27, 2014
211 (n) DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, as amended
212 (o) Joint Under Secretary of Defense for Intelligence, DoD Chief Information Officer, and
213 Commander, United States Strategic Command Memorandum, "Effective Integration of Cyber
214 and Traditional Security Efforts," March 31, 2014
215 (p) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999
216 (q) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010
217 (r) DoD Inspector General Report DODIG-2013-142, "DoD Evaluation of Over-Classification of
218 National Security Information," September 30, 2013
219 (s) DoDM 5200.02, "Procedures for the DoD Personnel Security Program," April 3, 2017, as
220 amended
221 (t) DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty
222 Organization Affairs (USSAN)," February 27, 2006
223 (u) United States Security Authority for NATO Affairs Instruction 1-07, "Implementation of North
224 Atlantic Treaty Organization (NATO) Security Requirements," April 5, 2007
225 (v) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008,
226 as amended
227 (w) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public
228 Release," August 13, 2014, as amended
229

230 ¹Available from the Central U.S. Registry
231
232

- 233 (x) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September
 234 11, 2012
- 235 (y) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign
 236 Governments and International Organizations," June 16, 1992
- 237 (z) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
- 238 (aa) DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical
 239 Security Review Board (PSRB)," December 10, 2005, as amended
- 240 (ab) DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011
- 241 (ac) Executive Order 12968, "Access to Classified Information," August 2, 1995, as amended
- 242 Intelligence Community Directive 703, "Protection of Classified National intelligence, Including
 243 Sensitive Compartmental Information (SCI)," June 21 2013
- 244 (ad) Intelligence Community Directive 703, "Protection of Classified National intelligence,
 245 Including Sensitive Compartmental Information (SCI)," June 21 2013²
- 246 (ae) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
- 247 (af) Sections 3021, 3141, 3142, 3143, 3144, 1801(p) and 2673 of title 50, United States Code
- 248 (ag) Section 1011 of Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of
 249 2004," December 17, 2004
- 250 (ah) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as
 251 amended
- 252 (ai) Part 1045 of title 10, Code of Federal Regulations
- 253 (aj) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as
 254 amended
- 255 (ak) National Security Directive 42, "National Policy for the Security of National Security
 256 Telecommunications and Information Systems," July 5, 1990
- 257 (al) DoD Instruction 3305.13, "DoD Security Education, Training, and Certification," February 13,
 258 2014
- 259 (am) DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23,
 260 2012, as amended
- 261 (an) National Security Agency/Central Security Service Policy Manual 3-16, "Control of
 262 Communications Security (COMSEC) Material," August 5, 2005
- 263 (ao) DoD Instruction 1100.22, "Policy and Procedures for Determining Workforce Mix," April 12,
 264 2010, as amended
- 265 (ap) Office of Federal Procurement Policy Letter 11-01, "Performance of Inherently Governmental
 266 and Critical Functions," September 12, 2011
- 267 (aq) Section 2011, et seq, of title 42, United States Code (also known as "The Atomic Energy Act
 268 of 1954, as amended")
- 269 (ar) DoD Directive 5210.48, "Credibility Assessment (CA) Program," April 24, 2015, as amended
- 270 (as) DoD Instruction 5210.02, "Access to and Dissemination of Restricted Data and Formerly
 271 Restricted Data," June 3, 2011, as amended
- 272 (at) DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special
 273 Access Programs (SAPs)," February 6, 2013

274
 275 ²Available from the Office of the Director of National Intelligence

276 ³Available on SIPRNET at

277 http://www.iad.nsa.smil.mil/resources/library/natl_pols_dirs_orders_section/index.cfm

278 ⁴CUI document, available to authorized users. Contact NSA/CSS Office of Corporate Policy
 279 (DJP1) for assistance

280

- 281 (au) Chairman of the Joint Chiefs of Staff Instruction 3231.01B, “Safeguarding Nuclear Command
282 and Control Extremely Sensitive Information,” June 21, 2006
- 283 (av) Chapters 21, 22, 31, 33, and 35 of title 44, United States Code
- 284 (aw) DoD Instruction 5015.02, “DoD Records Management Program,” February 24, 2015, as
285 amended
- 286 (ax) Sections 801-940 of title 10, United States Code (also known as “The Uniform Code of
287 Military Justice”)
- 288 (ay) Sections 102, 105, 552, and 552a of title 5, United States Code
- 289 (az) DoD Directive 5000.01, “The Defense Acquisition System,” May 12, 2003
- 290 (ba) DoD Instruction 5000.02, “Operation of the Defense Acquisition System,” 7, 2015, as
291 amended
- 292 (bb) DoD Instruction 5200.39, “Critical Program Information (CPI) Identification and Protection
293 within Research, Development, Test, and Evaluation (RDT&E),” May 28, 2015, as amended
- 294 (bc) DoD Instruction 3204.01, “DoD Policy for Oversight of Independent Research and
295 Development (IR&D),” August 20, 2014
- 296 (bd) Sections 181 through 188 of title 35, United States Code (also known as “The Patent Secrecy
297 Act of 1952, as amended”)
- 298 (be) DoD Directive 5230.25, “Withholding of Unclassified Technical Data from Public
299 Disclosure,” November 6, 1984, as amended
- 300 (bf) Section 1041 of Public Law 106-65, “National Defense Authorization Act for Fiscal Year
301 2000,” October 5, 1999
- 302 (bg) Section 3161 of Public Law 105-261, “Strom Thurmond National Defense Authorization Act
303 for Fiscal Year 1999,” October 17, 1998, as amended (also known as “The Kyl-Lott
304 Amendment”)
- 305 (bh) Presidential Memorandum, “Implementation of the Executive Order, ‘Classified National
306 Security Information,’” December 29, 2009
- 307 (bi) Executive Order 12951, “Release of Imagery Acquired by Space-Based National Intelligence
308 (bj) Reconnaissance Systems,” February 22, 1995
- 309 (bj) DoD 7000.14-R, Volume 11A, “Department of Defense Financial Management Regulation
310 (FMR): Reimbursable Operations Policy,” current edition
- 311 (bk) DoD Instruction 3200.12, “DoD Scientific and Technical Information Program (STIP),”
312 August 22, 2013
- 313 (bl) Executive Order 12958, “Classified National Security Information,” April 17, 1995, as
314 amended
- 315 (bm) DoD Manual 5200.45, “Instructions for Developing Security Classification Guides,” April 2,
316 2013
- 317 (bn) DoD 5400.7-R, “DoD Freedom of Information Act Program,” September 4, 1998, as amended
- 318 (bo) Public Law 116-92, “National Defense Authorization Act for Fiscal Year 2020,” December
319 20, 2019

321 5 This document is CUI. It is available to authorized recipients at
322 https://ca.dtic.mil/cjcs_directives/index.htm

323 6 Chapter 22 is also known as “The Presidential Records Act of 1978.”

324 7 Section 552 is also known as “The Freedom of Information Act, as amended.”

325 8 Section 552a is also known as “The Privacy Act of 1974, as amended.”

326
327
328

...

- 329 (bp) (Added)(DAF) DAFI 33-360, "Publications and Forms Management," December 1, 2015
 330 (correction August 7, 2021)
- 331 (bq) (Added)(DAF) AFI 33-322, "Records Management and Information Governance
 332 Program," March 23, 2020 (correction July 28, 2021)
- 333 (br) (Added)(DAF) AFI 16-701, "Management, Administration and Oversight of Special
 334 Access Programs," February 18, 2014
- 335 (bs) (Added)(DAF) AFI 16-1402, "Counter-Insider Threat Program Management," June 17,
 336 2020
- 337 (bt) (Added)(DAF) AFPD 16-14, "Security Enterprise Governance," December 31, 2019
- 338 (bu) (Added)(DAF) AFPD 16-1401, "Information Protection," July 29, 2019
- 339 (bv) (Added)(DAF) AFI 90-201, "The Air Force Inspection System," November 20, 2018
- 340 (bw) (Added)(DAF) DoDD 8100.02, "Use of Commercial Wireless Devices, Services, and
 341 Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April
 342 14, 2004
- 343 (bx) (Added)(DAF) DoDI5200.48_DAFI16-1403, "Controlled Unclassified Information,"
 344 October 5, 2021
- 345 (by) (Added)(DAF) Secretary of the Air Force (SecAF) Memorandum, "Delegation of
 346 Authority as Chief Information Officer under USC § 3506," February 5, 2021

347

348

349 *(Added)(DAF) ADOPTED FORMS

350

351 (Added)(DAF) AF Form 847, *Recommendation for Change of Publication*352 (Added)(DAF) DD Form 254, *Department of Defense Contract Security Classification*353 *Specification*354 (Added)(DAF) Standard Form (SF) 311, *Agency Information Security Program Data*355 (Added)(DAF) SF 312, *Classified Information Nondisclosure Agreement*356 (Added)(DAF) SF 700, *Security Container Information*357 (Added)(DAF) SF 701, *Activity Security Checklist*358 (Added)(DAF) SF 702, *Security Container Check Sheet*

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

...

377
378
379 ENCLOSURE 2

380
381 RESPONSIBILITIES

382
383
384 1. USD(I&S). The USD(I&S) shall:

385
386 a. Serve as the DoD Senior Security Official, in accordance with Reference (a), and in that
387 capacity is the DoD Senior Agency Official (SAO) appointed pursuant to subsection 5.4(d) of
388 Reference (d) to direct, administer, and oversee the DoD Information Security Program.

389
390 b. Notify Congress and the Director, Information Security Oversight Office (ISOO), as
391 appropriate, of violations involving classified information and of approval of waivers involving
392 Reference (d) and its implementing directive, reference (f)), required by section 2723 of title 10,
393 United States Code (U.S.C.) (Reference (l)) and References (d) and (f).

394
395 c. Establish requirements for collecting and reporting data, as necessary, to fulfill the
396 requirements of References (d) and (f) and other national-level guidance.

397
398 d. Designate a senior-level Federal employee, and an alternate, to represent the DoD on the
399 Interagency Security Classification Appeals Panel (ISCAP), as required by Reference (d). The
400 individuals, so designated, must be full-time or permanent part-time employees of the DoD.
401 Designate to the ISCAP Chair, in writing, one or more individuals as identified by the Director,
402 Washington Headquarters Services (WHS) to serve as a liaison in support of the DoD
403 representative in accordance with the ISCAP bylaws in Reference (f).

404
405 e. Establish policy and oversee program implementation for reporting and investigating known
406 or suspected incidents of unauthorized disclosure of classified information and controlled
407 unclassified information (CUI) for reporting corrective and disciplinary action taken in accordance
408 with DoDD 5210.50 (Reference (m)).

409
410 f. Serve as the principal point of contact on counterintelligence (CI) and security investigative
411 matters that involve the unauthorized disclosure of classified information and CUI referred to the
412 DoD by other government agencies or that may involve other government agencies, in accordance
413 with Reference (m).

414
415 g. Develop and oversee policy, strategy, plans, programs, required capabilities and resources
416 for DoD intelligence, CI, security, sensitive activities, and other intelligence and security related
417 matters, as necessary to counter insider threats. Serves as the senior official and principal advisor
418 to the Secretary of Defense on the DoD Insider Threat program in accordance with DoDD 5205.16
419 (Reference (n)), and in this capacity, will:

420
421 (1) Provide oversight of the DoD Insider Threat Program.

422
423 (2) Assign responsibilities to the DoD Components to implement the DoD Insider Threat
424 Program.

...

425
426 (3) Recommend improvements to the Secretary of Defense on DoD insider threat
427 activities.

428
429 h. In coordination with the DoD Chief Information Officer (DoD CIO), the Chairman of the
430 Joint Chiefs of Staff, the DoD Component heads, and the DNI, develop and integrate traditional
431 and cyber security risk-based strategies and phased approaches to measurably increase DoD's
432 security posture against insider threats, in accordance with the joint USD(I&S), DoD CIO, and
433 Commander, United States Strategic Command Memorandum (Reference (o)).

434
435 i. ***(Added)(DAF) The Secretary of the Air Force, Administrative Assistant (SAF/AA)**
436 **serves as the senior official, providing oversight and assigning responsibilities for the DAF**
437 **counter-insider threat program. The Director, Security, Special Program Oversight and**
438 **Information Protection Division (SAF/AAZ) implements the DAF counter-insider threat**
439 **program, in accordance with Air Force Instruction (AFI) 16-1402, *Counter-Insider Threat***
440 ***Program Management* (reference (bs)).**

441
442
443 2. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) shall:

444
445 a. Serve as the senior official responsible for administering that portion of the DoD
446 Information Security Program pertaining to the National Classified Military Information Disclosure
447 Policy, foreign government (including North Atlantic Treaty Organization (NATO)) information,
448 and security arrangements for international programs in accordance with DoDD 5111.1 (References
449 (p) and (a)).

450
451 (1) **(Added)(DAF) The Deputy Under Secretary of the Air Force, International Affairs**
452 **(SAF/IA) is designated as the DAF disclosure authority, in accordance with Air Force Policy**
453 **Directive (AFPD) 16-2, *Disclosure of Military Information to Foreign Governments and***
454 ***International Organizations*.**

455
456 (2) ***(Added)(DAF) The Deputy Chief of Staff for Intelligence, Surveillance,**
457 **Reconnaissance (ISR) and Cyber Effects Operations (AF/A2/6), serves as the DAF principal**
458 **member on the Military Intelligence Disclosure Policy Committee, in accordance with**
459 **reference (bt); and, Directorate of Integrated Air, Space, Cyberspace, and ISR Operations**
460 **(SF/S2) serves as the Head of the Intelligence Community Element for the USSF, in**
461 **accordance with *Joint Designation of the United States Space Force Intelligence Element as a***
462 ***Member of the United States Intelligence Community, 8 January 2021.***

463
464 b. Notify the Director, ISOO, of approval of waivers involving Reference (d) and its
465 implementing directive, Reference (f).

466
467
468 3. DoD CIO. The DoD CIO shall:

469
470 a. Establish procedures, consistent with References (d) and (f) and this Manual, to ensure that
471 information systems, including networks and telecommunications systems, that process,
472 disseminate, or store classified information:

...

- 473
474 (1) Prevent access by unauthorized persons;
475
476 (2) Assure the integrity of the information; and
477
478 (3) Use, to the maximum extent practicable, common information technology (IT)
479 standards, protocols, interfaces, and standardized electronic formats to maximize availability and
480 authorize access.

481
482 b. Direct the use of technical means to prevent unauthorized copying of classified data and for
483 anomaly detection to recognize unusual patterns of accessing, handling, downloading, and removal
484 of digital classified information.

485
486
487 4. ADMINISTRATOR, DEFENSE TECHNICAL INFORMATION CENTER (DTIC). The
488 Administrator, DTIC, under the authority, direction, and control of the Under Secretary of Defense
489 for Acquisition, Technology, and Logistics and in addition to the responsibilities in section 6 of this
490 enclosure, shall maintain an index of security classification guides (SCGs) in an online database,
491 accessible through www.dtic.mil.

492
493
494 5. DIRECTOR, WHS. The Director, WHS, under the authority, direction, and control of the Chief
495 Management Officer of the DoD, through the Director of Administration, shall identify to the
496 USD(I&S) an individual and at least one alternate to serve as the ISCAP liaison for the DoD in
497 accordance with the ISCAP bylaws in Reference (f).

498
499
500 6. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall, in
501 accordance with Reference (b):

502
503 a. Be responsible for the overall management, functioning, and effectiveness of the
504 information security program within their respective DoD Component.

505
506 b. Appoint a Senior Agency Official (SAO) to be responsible for directing, administering, and
507 overseeing the information security program, within the Component, on his or her behalf and
508 ensure that this official accomplishes the responsibilities identified in section 7 of this enclosure.
509 The DoD Component Head may designate a separate senior official to be responsible for
510 overseeing SAPs within the Component, if necessary, in accordance with DoDD 5205.07
511 (Reference (q)).

512
513 c. If the Component is not an element of the Intelligence Community, designate a Senior
514 Intelligence Official (SIO) to be responsible for ensuring adequate funding and effective
515 implementation of the component's SCI security program, including awareness and education,
516 consistent with guidance established by the DNI.

517
518 d. Identify, program for, and commit necessary resources to effectively implement the
519 requirements for protection of classified information, as part of the component's information
520 security program.

...

521
522 e. Conduct, as periodically directed by the USD(I&S), reviews of the DoD component's
523 classification guidance and provide reports summarizing results.

524
525 f. Ensure the component SAO and SIO coordinate, as appropriate, to achieve a harmonized
526 and cohesive information security program.

527
528 **g. (Added)(DAF) SAF/AA is the DAF SAO, responsible for oversight of information**
529 **security program, in accordance with reference (bt). SAF/AA also serves as the DAF Security**
530 **Program Executive, representing the DAF security enterprise on the Defense Security**
531 **Enterprise Executive Committee.**

532
533 **h. (Added)(DAF) AF/A2/6 serves as the Head of the Intelligence Community Element**
534 **and is responsible for all actions regarding the security, use, and dissemination of SCI,**
535 **consistent with HAF Mission Directive (HAFMD) 1-33, Deputy Chief of Staff of the Air Force,**
536 **Intelligence, Surveillance and Reconnaissance.**

537
538 **i. (Added)(DAF) The Deputy Chief of Staff, Strategic Deterrence and Nuclear**
539 **Integration (AF/A10) is the HAF Restricted Data Management Official for the nuclear**
540 **information security program, consistent with HAFMD 1-60, Deputy Chief of Staff of the Air**
541 **Force Strategic Deterrence and Nuclear Integration. AF/A10 will:**

542
543 **(1) (Added)(DAF) Provide subject matter expertise on the classification and/or**
544 **declassification of Restricted Data (RD), Formerly Restricted Data (FRD), Controlled**
545 **Nuclear Weapons Design information (CNWDI), Department of Energy (DOE) Sigma**
546 **information, and Transclassified Foreign Nuclear Information (TFNI).**

547
548 **(2) *(Added)(DAF) Review classification challenges and security incidents involving**
549 **RD or FRD and report to the appropriate information owners.**

550
551 **(3) (Added)(DAF) Serve as the gatekeeper for DAF personnel requiring access to**
552 **DOE Sigma nuclear weapons data. Notify the Air Force Personnel Center to ensure a**
553 **permanent assignment limitation code is applied to personnel records who have been granted**
554 **access to Sigma 14. Subsequently, execute waiver authority for assignment limitation code**
555 **removal, in accordance with DAFI 36-2110, Total Force Assignments.**

556
557 **(4) *(Added)(DAF) Coordinate on the development and dissemination of SCGs**
558 **containing nuclear weapons information, developed by DOE and/or other DoD offices, which**
559 **are intended for use by DAF field activities.**

560
561 **(5) *(Added)(DAF) The Commander, Headquarters United States Air Forces Global**
562 **Strike Command shall support AF/A10, by developing, coordinating, promulgating,**
563 **implementing, and evaluating DAF nuclear information security program policy and**
564 **procedures.**

565
566 **j. (Added)(DAF) The Deputy Chief of Staff, Logistics, Engineering and Force Protection**
567 **(AF/A4) serves as the DAF OPR for DoD unclassified controlled nuclear information (UCNI).**
568 **AF/A4 has final authority on whether documents contain, do not contain, or no longer**

569 **contain DoD UCNI.**

570
571 **k. (Added)(DAF) The Information Management Directorate (SAF/AAI) serves as the**
572 **lead for the DAF declassification program.**

573
574
575 7. SENIOR AGENCY OFFICIALS. The SAO, under the authority, direction, and control of the
576 Heads of the DoD Component, is appointed in accordance with section 6 of this enclosure shall, in
577 addition to the responsibilities in DoDI 5200.48 for CUI, will:

578
579 a. Direct, administer, and oversee their respective Component's information security program.

580
581 b. Develop guidance, as necessary, for program implementation within the DoD Component.

582
583 c. Direct the head of each activity, within the DoD Component, that creates, handles, or stores
584 classified information to appoint, in writing, an official to serve as security manager for the activity,
585 to properly manage and oversee the activity's information security program. Persons appointed to
586 these positions shall be provided training, as Enclosure 5 of Volume 3 of this Manual requires.

587
588 d. Establish and maintain an ongoing self-inspection and oversight program to evaluate and
589 assess the effectiveness and efficiency of the DoD Component's implementation of that portion of
590 the information security program pertaining to classified information.

591
592 (1) Evaluation criteria shall consider, at a minimum, original and derivative classification,
593 declassification, safeguarding, security incidents, education and training, and management and
594 oversight.

595
596 (2) The program shall include regular reviews and assessments of representative samples of
597 the DoD Component's classified products. Appropriate officials shall be authorized to correct
598 misclassification of information, except for information covered by paragraph 17.b. or section 18 of
599 Enclosure 4 of this Volume.

600
601 (3) Self-inspections shall be conducted at least annually, with the frequency established
602 based on program needs and classification activity. DoD Component activities that originate
603 significant amounts of classified information should be inspected at least annually. Annual reports
604 on the Component's self-inspection program shall be submitted, as required, by ISOO and/or
605 USD(I&S). The report shall include:

606
607 (a) A description of the agency's self-inspection program, to include activities assessed,
608 program areas covered, and methodology utilized.

609
610 (b) A summary of the findings in the following program areas: original classification,
611 derivative classification, declassification, safeguarding, security violations, security education and
612 training, and management and oversight.

613
614 (c) Specific information on the findings of the annual review of agency original and
615 derivative classification actions to include the volume of classified material reviewed and the
616 number and type of discrepancies that were identified.

...

617
618 (d) Actions taken or planned to correct identified deficiencies or misclassification
619 actions, and to deter their recurrence.

620
621 (e) Best practices identified. The DoD Inspector General Report DODIG-2013-142
622 (Reference (r)) identifies examples of DoD Component best practices, including the following:

623
624 1. Using Microsoft SharePoint® to make available all information that security
625 managers need to manage their programs and share unit best practices.

626
627 2. Creating and using an electronic security manager handbook.

628
629 3. Providing and maintaining open communications between different levels of
630 management structure within the organization.

631
632 4. Establishing and using online training tools to track training requirement
633 completion.

634
635 5. Issuing and using a quarterly security newsletter that provides information
636 security articles, security updates, and upcoming security courses.

637
638 6. Maintaining an automated security incident reporting program.

639
640 7. Maintaining complete inventories of all classified documents and electronic
641 media to provide precise tracking of classified holdings.

642
643 8. Developing organization-level derivative classification training.

644
645 9. Reviewing the process for public release of information.

646
647 10. Maintaining a central security and education awareness mailbox with questions
648 answered by close of business.

649
650 11. Tracking mandatory annual security and derivative classification training by
651 the human resources information system of record, which enhances better oversight of training
652 completion rates.

653
654 12. Developing a comprehensive security database reflecting final adjudication
655 and investigation of security incidents.

656
657 **(4) (Added)(DAF) An annual information security program compliance inspection**
658 **consists of the servicing IP office analyzing the supported activity's information security**
659 **metrics, data systems, inspection reports, inventory controls, requests for assistance, and**
660 **Management Internal Control Toolset (MICT) self-assessment checklists (SACs). Annual**
661 **ISOO or USD (I&S) information security reports will not supplant DAF activities from**
662 **conducting annual self-inspections. (T-0).**

663
664 **(a) (Added)(DAF) Commanders/directors must ensure annual self-assessments**

...

665 are completed, as defined in AFI 90-201, *The Air Force Inspection System* (reference (bv)). (T-
666 1).

667
668 **(b) (Added)(DAF) The Chief, IP will validate completion of annual self-**
669 **assessments by supported activities, in MICT. (T-1).**

670
671 e. Establish procedures to prevent unauthorized persons from accessing classified information,
672 including:

673
674 (1) Specific requirements for protecting classified information at DoD Component-
675 sponsored meetings and conferences, to include seminars, exhibits, symposiums, conventions,
676 training activities, workshops, or other such gatherings, during which classified information is
677 disseminated.

678
679 (2) Requirements for protecting U.S. classified information located in foreign countries,
680 with particular attention on ensuring proper enforcement of controls on release of U.S. classified
681 information to foreign entities.

682
683 (3) Procedures to accommodate visits to DoD Component facilities involving access to, or
684 disclosure of, classified information.

685
686 (4) Establish and maintain declassification programs and plans that meet the requirements
687 of this Manual and ensure that necessary resources are applied to the review of information to
688 ensure it is neither classified for longer than necessary nor declassified prematurely.

689
690 (5) Establish and maintain a security education and training program as required by
691 Enclosure 5 of Volume 3 of this Manual, ensure that DoD Component personnel receive security
692 education and training as appropriate to their functions, and grant, when appropriate, waivers to the
693 original and derivative classification training requirements of section 7 of Enclosure 5 of Volume 3.

694
695 f. Ensure that the performance contract or other system used to rate the performance of civilian
696 and military personnel includes the designation and management of classified information, to
697 include Restricted Data (RD) and Formerly Restricted Data (FRD) information, when appropriate,
698 as a critical element or item to be evaluated in the rating of:

699
700 (1) Original classification authorities (OCAs).

701
702 (2) Security managers and security specialists.

703
704 (3) Personnel who derivatively classify information on a routine basis.

705
706 (4) Information system security personnel if their duties involve access to classified
707 information and information system personnel (e.g., system administrators) with privileged access
708 to classified system or network resources.

709
710 (5) All other personnel whose duties include significant involvement with the creation or
711 handling of classified information.

712

713 g. Account for the costs associated with implementing this Manual within the DoD
714 Component and report those costs as required.

715
716 h. Ensure prompt and appropriate response to any request, appeal, challenge, complaint, or
717 suggestion arising out of implementation of this Manual within the DoD Component.

718
719 i. Establish procedures for receipt of information, allegations, or complaints regarding over-
720 classification or incorrect classification within the DoD Component and, as needed, provide
721 guidance to personnel on proper classification.

722
723 j. Approve, when appropriate, the use of alternative compensatory control measures (ACCM)
724 for classified information over which the SAO has cognizance and provide written notification
725 within 30 days to the Director of Security, Under Secretary of Defense for Intelligence
726 (USD(I&S)), or the Director, International Security Programs, Defense Technology Security
727 Administration, USD(P), as appropriate, when establishing or terminating an ACCM.

728
729 k. Submit an annual report addressing how the DoD Component implemented that portion of
730 the information security program dealing with classified information.

731
732 (1) The report, covering the previous fiscal year, shall be submitted on Standard Form (SF)
733 311, "Agency Information Security Program Data," to reach the Director of Security, USD(I&S),
734 prior to October 31 of each year. The Military Departments shall submit their reports directly to
735 ISOO, with a copy furnished to USD(I&S). USD(I&S) shall compile the reports, excluding those
736 of the Military Departments, and provide a consolidated report to ISOO.

737
738 (2) The ISOO self-inspection report shall be completed according to the instructions
739 accompanying the form and those provided by ISOO and USD(I&S).

740
741 l. Submit to the Director of Security, USD(I&S), prior to October 31 of each year, a report
742 listing, by position title, those officials within the DoD Component who hold OCA delegated in
743 accordance with paragraph 4.c. of Enclosure 4 and those officials who hold declassification
744 authority delegated in accordance with paragraph 3.b. of Enclosure 5. The report shall be organized
745 by level of highest classification authority and by activity.

746
747 m. Cooperate and coordinate with the Component SIO, as appropriate, to achieve a
748 harmonized and cohesive information security program within the DoD Component.

749
750 **n. *(Added)(DAF) DAF INFORMATION SECURITY PROGRAM**

751
752 **(1) (Added)(DAF) SAF/AAZ**

753
754 **(a) (Added)(DAF) Administers and oversees the information security program,**
755 **as designated by the SAO, in accordance with reference (bu).**

756
757 **(b) (Added)(DAF) Serves as the Director, DAF Special Access Program Central**
758 **Office (SAPCO), responsible for developing policies and procedures as it pertains to the**
759 **management, administration and oversight of SAPs.**

760
761 **(c) *(Added)(DAF) At this time, SAF/AAZ only provides administrative**

oversight for ACCM policy within the DAF, as the DAF does not have cognizance over any active ACCMs. If DAF personnel support ACCMs established by another activity, they must abide by the security requirements provided by the cognizant ACCM sponsor, in accordance with Enclosure 2, of Volume 3, to this Manual.

(2) *(Added)(DAF) The MAJCOM/FLDCOM commander will appoint a Security Program Executive (SPE), in accordance with AFI 16-1401, *Information Protection* (reference (bu)). (T-1). The SPE should be a senior-level person within the organization, with the ability and access to resources to adequately administer and oversee the program.

(3) (Added)(DAF) The SPE will:

(a) *(Added)(DAF) Administer and oversee the MAJCOM/FLDCOM information security program, by enforcing adherence to prescribed standards for marking, safeguarding, storing, destroying, transmitting, and transporting records containing classified information. (T-1).

(b) *(Added)(DAF) Serve as the approval authority on the removal of records containing secret and confidential information from designated work areas, for use at an uncleared residence (i.e., residential storage). Top secret residential storage requests must be submitted to the DAF SAO, via SAF/AAZ. (T-0).

(c) *(Added)(DAF) Implement a mandatory declassification review (MDR) program, to support the Administrative Assistant to the Secretary of the Air Force, Information Management Directorate, Policy and Chief Information Officer Support Division (SAF/AII), by appointing a primary and alternate MDR monitor, in writing. (T-1). Appointment letters must be sent to:

1. saf.aa.mdr.workflow@us.af.mil; or,

2. SAF/AII (MDR)
1000 Air Force Pentagon
Washington DC, 20330-1000

(d) (Added)(DAF) Approve or make recommendations, as appropriate, regarding waivers, exceptions, or deviations to policy and submit them to the appropriate organizational entity, as required. (T-1).

(4) (Added)(DAF) The MAJCOM/FLDCOM Director, Information Protection will:

(a) (Added)(DAF) Administer the information security program, on behalf of the SPE, and develop guidance for program implementation within MAJCOM/FLDCOM operations. (T-1).

(b) (Added)(DAF) Provide oversight, direction and training to staff security specialists for the efficient and effective implementation of the information security program. (T-1).

810 (c) (Added)(DAF) Chair, or participate in, SPE-designated forums to address
811 information security concerns. (T-1).

812
813 (d) (Added)(DAF) Ensure supplements to DAF security policies are coordinated
814 through SAF/AAZ for concurrence. (T-1).

815
816 (e) (Added)(DAF) Develop and maintain a system to track security incident
817 (violations and infractions) metrics and report them to the SPE and/or SAF/AAZ, as
818 required. (T-1). The matrix at appendix 3, to enclosure 6, of volume 3 will serve as the
819 minimum requirement for capturing these metrics. (T-0).

820
821 (f) (Added)(DAF) Review staff packages for SPE endorsement, on requests to
822 remove confidential and/or secret classified information for work at home, for mission critical
823 occurrences. (T-1).

824
825 (g) (Added)(DAF) Assess requests for waivers, exceptions, or deviations to policy
826 and validate the accuracy prior to endorsement by the SPE and submission to the
827 appropriate organizational entity, as required. (T-1).

828
829 (h) *(Added)(DAF) Establish a process to validate original classification
830 authority (OCA) delegations annually, at minimum. (T-1). Review and endorse the training
831 materials (or job aids) utilized to conduct initial and refresher OCA training. (T-1).

832
833 (i) *(Added)(DAF) Ensure supported activities establish an inspection program
834 to validate and verify supported activities' information security program. At minimum, the
835 continual evaluation process should identify findings, determine root causes, apply corrective
836 actions, ensure follow up, and share results, per reference (bv). (T-1). This includes, but is
837 not limited to:

838
839 (j) (Added)(DAF) Validate wing IP offices are completing annual SACs in MICT
840 and addressing deficiencies. (T-1).

841
842 (k) (Added)(DAF) Collect ISOO annual self-inspection reports from the wings
843 and submit a consolidated report to SAF/AAZ. (T-1).

844
845 (5) (Added)(DAF) The wing (installation) commander will:

846
847 (a) (Added)(DAF) Direct, administer and oversee the information security
848 program. This may be delegated, in writing, to the Vice (or Deputy) commander. (T-1).

849
850 (b) (Added)(DAF) Appoint a Chief of Information Protection (Chief, IP) and
851 establish an IP office, which reports directly to wing commander (CC) or vice commander
852 (CV). (T-1).

853
854 (c) *(Added)(DAF) Staff the wing IP office with properly trained government
855 security specialists (Office of Personnel Management – 0080 series), to administer the
856 program. Contractors within the wing IP office can only assist with the development of
857 security procedures, plans, and forms (i.e., cannot perform inherently government roles and

858 responsibilities). (T-1).

859

860 (d) *(Added)(DAF) If the command creates, stores or handles RD, FRD, CNWDI,
861 DOE Sigma information, or TFNI, as defined in DoDI 5210.02, *Access to and Dissemination of*
862 *Restricted Data and Formerly Restricted Data*, designate an associate RD Management
863 Official, in writing. (T-0). For the aforementioned information, the RD management official
864 will:

865

866 1. (Added)(DAF) Disseminate implementing directives and nuclear
867 classification guidance. (T-1).

868

869 2. (Added)(DAF) Ensure U.S. government and contractor-support
870 personnel are trained on the procedures for derivative classification principles. (T-1).

871

872 3. (Added)(DAF) Verify access and certify prescribed indoctrination and
873 annual training requirements are being met. (T-1).

874

875 4. (Added)(DAF) Establish local protocols and continuously validate that
876 controls are in place. (T-1).

877

878 5. (Added)(DAF) Coordinate with AF/A10 for any security incidents,
879 classification challenges or declassification. (T-1).

880

881 (e) *(Added)(DAF) If the wing creates, stores or processes NATO information,
882 ensures that the installation/wing has a servicing NATO sub-registry (or control point).
883 Ensure NATO accountability, controls and security procedures are followed in accordance
884 with DoDD 5100.55, *USSAN Instruction 1-07*, and enclosure 2 of this volume. (T-0).

885

886 (f) (Added)(DAF) Make security-in-depth and supplemental control
887 determinations, as warranted. (T-1).

888

889 (g) *(Added)(DAF) Establish an inspection program to evaluate the effectiveness
890 and efficiency of the supported activities' information security program. (T-1). Corrective
891 action plans must be continuously monitored in MICT or Inspector General Evaluation
892 Management System (IGEMS), until all deficiencies have been remedied. (T-1). Appointing
893 a representative from the IP office to accompany the wing inspection team is highly
894 recommended.

895

896 (h) *(Added)(DAF) Ensure secure rooms (i.e., open storage area) are certified
897 and revalidated, as required; this can be delegated to the Chief, Wing IP. (T-1).

898

899 1. *(Added)(DAF) In spaces where classified information is being stored or
900 processed, which do not meet secure room requirements, the space custodian must:

901

902 a. *(Added)(DAF) Adhere to the minimum storage requirements
903 identified in Volume 3, of this Manual, as well as any local policies or procedures; and

904

905 b. *(Added)(DAF) Coordinate with the servicing IP and cybersecurity

906 offices, prior to installing a classified information system/network.

907
908 (i) *(Added)(DAF) Verify measures are in place to protect classified information
909 aboard aircraft and other military platforms, away from the home-station. (T-1). Moreover,
910 address specific measures taken to manage any risks to classified information on aircraft in
911 foreign countries, where non-U.S. security support is provided. (T-1).

912
913 (6) (Added)(DAF) The wing (installation) Chief, IP will:

914
915 (a) *(Added)(DAF) Serve as the activity security manager. Perform duties
916 identified in Enclosure 2, Paragraph 9 (below), as well as AFI 16-1401, *Information*
917 *Protection*. (T-1). Duties may be tailored to meet the organization's needs. Contractors
918 cannot be appointed as an activity security manager. (T-0).

919
920 1. *(Added)(DAF) Activity security managers, assistant security managers
921 and security assistants must be trained in accordance with Volume 3, Enclosure 5 of this
922 Manual. (T-0). Mandatory training must be completed within 6 months of appointment. (T-
923 0).

924
925 (b) *(Added)(DAF) Evaluate the effectiveness and efficiency of the supported
926 activities' information security program, in accordance with Enclosure 2, paragraph 7d. (T-
927 1). This includes:

928
929 1. (Added)(DAF) Reviewing MICT SACs and communicating with wing
930 leadership on the health of the information security program. (T-1).

931
932 2. (Added)(DAF) Using the data collected from supported activities' annual
933 information self-inspections to prepare the wing's ISOO annual self-inspection report and
934 submit a final copy to the MAJCOM/FLDCOM IP office. (T-1).

935
936 3. (Added)(DAF) Going over supplemental security instructions, processes
937 and procedures to ensure the following areas are covered (at minimum). (T-1).

938
939 a. (Added)(DAF) Provisions for safeguarding classified information
940 during emergency situations and military operations, if appropriate.

941
942 b. (Added)(DAF) Security measures and procedures regarding visitors
943 who require access to classified information or facilities that contain classified information.

944
945 c. (Added)(DAF) Identification of a classified storage location for
946 personnel arriving unexpectedly or while in transit and in possession of classified
947 information.

948
949 d. (Added)(DAF) Procedures for the protection, removal or destruction
950 of classified material during emergency situations (e.g., fire, natural disaster, civil
951 disturbance, etc.).

952
953 e. (Added)(DAF) Guidance on the use of government or personal

...

954 portable electronic devices (PEDs) (e.g., cellphones, fitness trackers, MP3 players, smart
 955 watches, wireless two-way devices, etc.); medical devices (i.e., hearing aids, breast pumps,
 956 etc.); and devices that have photographic or audio recording capabilities in areas where
 957 classified information is discussed or processed.

958
 959 **f. (Added)(DAF) Procedures for conducting end-of-day security checks**
 960 **at the close of each duty or business day, to ensure classified information is secure within unit**
 961 **work centers. The SF 701, *Activity Security Checklist*, will be utilized to conduct these checks.**
 962 **(T-0).**

963
 964 **g. (Added)(DAF) Procedures on identifying, marking and utilizing**
 965 **equipment used for reproducing classified information and ensuring the systems are**
 966 **accredited properly. The approval must facilitate oversight and control of the reproduction**
 967 **of classified information and the use of the equipment for such reproduction. (T-0).**

968
 969 **h. (Added)(DAF) Creates processes to ensure personnel with knowledge**
 970 **of combinations to security containers, secure rooms and vaults are maintained and**
 971 **combinations are changed in accordance with volume 3, enclosure 3 of this Manual.**

972
 973 **i. (Added)(DAF) Procedures for hosting classified meetings and**
 974 **conferences.**

975
 976 **(c) (Added)(DAF) Develop procedures for the establishment and recertification**
 977 **of secure rooms. (T-1).**

978
 979 **1. *(Added)(DAF) The local cybersecurity office must validate the space is**
 980 **accredited to process classified information for each classified information system. (T-1).**

981
 982 **2. *(Added)(DAF) Spaces not designated as a secure room must store**
 983 **classified material in a General Service Administration (GSA)-approved security container,**
 984 **when it is not under personal observation or control. (T-0).**

985
 986 **(d) *(Added)(DAF) Establish a system to track OCA delegation letters and**
 987 **training certifications, if assigned. (T-0). Ensure unit training managers document this**
 988 **training, in accordance with DAFI 36-2670, *Total Force Development*.**

989
 990 **(7) (Added)(DAF) The commander or director will:**

991
 992 **(a) *(Added)(DAF) Establish and maintain a program to continually evaluate the**
 993 **effectiveness and efficiency of the information security program (i.e., MICT to monitor**
 994 **compliance; IGEMS for evaluation and self-assessments; and, the ISOO annual report). (T-**
 995 **1).**

996
 997 **1. *(Added)(DAF) Appoint a security manager or security assistant, based**
 998 **on operational needs. The use of contractors as a security assistant is acceptable, in**
 999 **accordance with AFI 16-1401 (T-1). However, they can only perform security-related duties**
 1000 **identified in Section 7, of this Enclosure. (T-1).**

1001

...

1002 **2. *(Added)(DAF) A combined approach, where one (1) security manager**
 1003 **(or assistant) services combined populations of organizationally aligned smaller units, groups**
 1004 **and staff agencies, rather than each unit having its own security manager (or assistant), can**
 1005 **be utilized.**

1006
 1007 **(b) *(Added)(DAF) Ensure local security instructions, plans and/or processes**
 1008 **include the minimum requirements identified at paragraph (6)(b)3, above. (T-1).**

1009
 1010 **(c) (Added)(DAF) Establish a SETA program. (T-1).**

1011
 1012 **(d) *(Added)(DAF) Ensure personnel who process classified information or**
 1013 **utilize classified information systems complete initial derivative classification training,**
 1014 **followed by annual refreshers thereafter, in accordance with volume 3, enclosure 5, of this**
 1015 **Manual. This includes ensuring training records are maintained by the security**
 1016 **representative, or a system of record. (T-1).**

1017
 1018 **(e) (Added)(DAF) Evaluate security incidents and work with the wing IP office to**
 1019 **determine appropriate mitigation measures are taken, to prevent further occurrences. (T-1).**

1020
 1021 **(f) *(Added)(DAF) Coordinate with the servicing cybersecurity office prior to**
 1022 **processing classified information on any information system, communications system or**
 1023 **cryptographic equipment. If utilizing leased equipment, develop a process to ensure hard**
 1024 **drives are properly sanitized or destroyed, prior to the end of the lease agreement. (T-1).**

1025
 1026 **o. (Added)(DAF) Air Force District of Washington (11th Wing/IP) is responsible for**
 1027 **overseeing the information security program for SecAF, HAF and HQ USSF staff**
 1028 **directorates.**

1029
 1030 **p. (Added)(DAF) The Headquarters, Air Force Operational Test and Evaluation Center**
 1031 **(AFOTEC) IP office maintains information security oversight of all assigned AFOTEC**
 1032 **headquarters agencies and geographically separated units.**

1033
 1034 **q. (Added)(DAF) The Deputy Chief of Staff, Manpower, Personnel and Services (AF/A1)**
 1035 **ensures civilian and military performance appraisal systems include the designation and**
 1036 **management of classified information as a critical element, or an item to be evaluated.**

1037
 1038
 1039 **8. HEADS OF DoD ACTIVITIES. The heads of DoD activities shall:**

1040
 1041 **a. Be responsible for overall management, functioning and effectiveness of the activity's**
 1042 **information security program.**

1043
 1044 **b. Designate, in writing, an activity security manager, who shall be given the necessary**
 1045 **authority to ensure personnel adhere to program requirements. Provide the designated activity**
 1046 **security manager direct access to activity leadership and ensure he or she is organizationally**
 1047 **aligned to ensure prompt and appropriate attention to program requirements.**

1048
 1049 **(1) The activity security manager may be assigned full-time, part-time, or as a collateral**

1050 duty, provided that the responsibilities delineated in Section 9 of this enclosure can be adequately
1051 and professionally executed and implemented.

1052
1053 (2) The activity security manager shall:

1054
1055 (a) Be a military officer, senior non-commissioned officer, or a civilian employee
1056 with sufficient authority, staff, and other resources necessary to manage the program for the
1057 activity.

1058
1059 1. For activities with more than 100 personnel assigned, a senior non-
1060 commissioned officer designated as the activity security manager shall be E-7 or above; a civilian
1061 employee so designated shall be GS-11 or above (or pay band equivalent).

1062
1063 2. For activities with less than 100 personnel assigned, a senior non-
1064 commissioned officer designated as the activity security manager shall be E-6 or above; a civilian
1065 employee so designated shall be GS-7 or above (or pay band equivalent).

1066
1067 (b) Be a U.S. citizen.

1068
1069 (c) Have been the subject of a favorably adjudicated, current background
1070 investigation appropriate for the highest level of classification of information handled by personnel
1071 within the activity in accordance with requirements of DoDM 5200.02 (Reference (s)).

1072
1073 (d) Have access appropriate to the level of information managed.

1074
1075 c. In large activities and where circumstances warrant, designate, in writing, activity assistant
1076 security manager(s) to assist in program implementation, maintenance, and local oversight.

1077
1078 (1) Responsibilities assigned to assistant security managers shall be commensurate with
1079 their grade level, experience, and training.

1080
1081 (2) Individuals assigned as assistant security managers shall be U.S. citizens with security
1082 clearances and accesses appropriate to their assigned responsibilities.

1083
1084 (3) Assistant security managers shall report directly to the activity security manager who
1085 shall provide guidance, direction, coordination, training, and oversight necessary to ensure that the
1086 program is being administered effectively.

1087
1088 d. Optionally, where circumstances warrant (such as in activities with large repositories of top
1089 secret information), designate an activity Top Secret Control Officer (TSCO) to manage and
1090 account for Top Secret materials, and Top Secret Control Assistant (TSCA), as needed, to assist the
1091 TSCO. When used, designations shall be in writing. Top secret couriers are NOT considered
1092 TSCA(s).

1093
1094 (1) An individual designated as the TSCO must have been the subject of a favorably
1095 adjudicated, current background investigation in accordance with requirements of Reference (s) and
1096 must have top secret access. The TSCO shall report directly to the activity security manager, or the
1097 activity security manager may serve concurrently as the TSCO.

...

1098
1099 (2) An individual designated as a TSCA must have been the subject of a favorably
1100 adjudicated, current background investigation, in accordance with requirements of Reference (s)
1101 and must have top secret access.

1102
1103 e. When required by DoDD 5100.55 (Reference (t)), designate, in writing, an activity NATO
1104 control point officer and at least one alternate to ensure that NATO information is correctly
1105 controlled and accounted for, and that NATO security procedures are followed. U.S. Security
1106 Authority for NATO (USSAN) Instruction 1-07 (Reference (u)) was written by USD(P) on behalf
1107 of the Secretary of Defense, acting as the U.S. Security Authority to NATO and administrator of
1108 NATO information security regulation. It establishes procedures and minimum security standards
1109 for the handling and protection of NATO classified information.

1110
1111
1112 9. ACTIVITY SECURITY MANAGER. The activity security manager shall:

1113
1114 a. Manage and implement the DoD activity's information security program on behalf of the
1115 activity head, to whom he or she shall have direct access.

1116
1117 b. Serve as the principal advisor and representative to the activity head in all matters
1118 pertaining to this Manual and maintain cognizance of all activity information, personnel,
1119 information systems, physical and industrial security functions to ensure that the information
1120 security program is coordinated in its execution and inclusive of all requirements in this Manual.

1121
1122 c. Provide guidance, direction, coordination, and oversight to designated assistant security
1123 managers, TSCOs, TSCAs, security assistants and, as appropriate, others in security management
1124 roles as necessary to ensure that all elements of the information security program are being
1125 administered effectively, efficiently, and in a coordinated manner.

1126
1127 d. Develop a written activity security instruction that shall include provisions for safeguarding
1128 classified information during emergency situations and military operations, if appropriate.

1129
1130 e. Ensure that personnel in the activity who perform security duties are kept abreast of changes
1131 in policies and procedures, and provide assistance in solving problems.

1132
1133 f. Formulate, coordinate, and conduct the activity security education and training program.
1134 Organizations with elements that are deployable for contingency operations shall ensure
1135 information security training, to include appropriate application to information systems, is an
1136 integral part of pre-deployment training and preparation.

1137
1138 g. Ensure that threats to security and security incidents pertaining to classified information,
1139 including foreign government information (FGI), are reported, recorded, coordinated with the
1140 proper authorities, and, when necessary, investigated and that appropriate action is taken to mitigate
1141 damage and prevent recurrence. Ensure that incidents involving the loss or compromise of
1142 classified material (as described in Enclosure 6 of Volume 3 of this Manual) are immediately
1143 referred to the cognizant investigative authority. In cases where compromise is determined or
1144 cannot be ruled out, ensure that security reviews and other required assessments are conducted as
1145 soon as possible. Coordinate with local information assurance officials, but retain responsibility for
1146 inquiries into incidents involving possible or actual compromise of classified information resident

1147 in or on IT systems.

1148
1149 h. Coordinate the preparation, dissemination, and maintenance of security classification guides
1150 under the activity's cognizance as required by Enclosure 6 of this Volume.

1151
1152 i. Maintain liaison with the activity public affairs officer or information security officer, as
1153 appropriate, and the operations security (OPSEC) officer to ensure that information, including press
1154 releases and photos, proposed or intended for public release, including via website posting, is
1155 subject to a security review in accordance with DoDD 5230.09 (Reference (v)), DoDI 5230.29
1156 (Reference (w)), and DoDI 8550.01 (Reference (x)).

1157
1158 j. Coordinate with other activity officials regarding security measures for the classification,
1159 safeguarding, transmission, declassification, and destruction of classified information.

1160
1161 (1) Coordinate as required with the foreign disclosure officer on all matters governing the
1162 disclosure of classified information to foreign governments and international organizations in
1163 accordance with DoDD 5230.11 (Reference (y)).

1164
1165 (2) Ensure implementation of and compliance with the requirements of this Manual for all
1166 uses of IT. Coordinate with information systems security personnel (e.g., Designated Approval
1167 Authorities (DAAs) and Information System Security Managers (ISSM)), as required, for the
1168 effective management, use and oversight of classified information in electronic form.

1169
1170 k. Develop security measures and procedures, consistent with DoDD 5230.20 (Reference (z)),
1171 DoDI 5200.08 (Reference (aa)) and other applicable policies, regarding visitors who require access
1172 to classified information and facilities containing same.

1173
1174 l. Ensure compliance with the requirements of this Manual when access to classified
1175 information is provided to industry at activity facilities and locations in connection with a classified
1176 contract. If the classified information is provided to industry at the contractor's facility, ensure
1177 compliance with the provisions of DoDI 5220.22 (Reference (ab)).

1178
1179 m. Ensure that access to classified information is limited to appropriately cleared personnel
1180 with a need to know as required by section 4.1 of Reference (d) and section 3.1 of E.O. 12968
1181 (Reference (ac)).

1182
1183 n. Maintain liaison with the SSO, as appropriate, on issues of common concern.

1184
1185
1186 10. TSCO. The TSCO, when designated in accordance with paragraph 8.d. of this enclosure, shall:

1187
1188 a. For paper documents and other physical media (e.g., disk drives and removable computer
1189 media), maintain a system of accountability (e.g., registry) to record the receipt, reproduction,
1190 transfer, transmission, downgrading, declassification, and destruction of top secret information, that
1191 is not SAP, SCI, and other special types of classified information.

1192
1193 b. Ensure that inventories of top secret information are conducted at least annually or more
1194 frequently when circumstances warrant.

...

1196
1197 11. SENIOR INTELLIGENCE OFFICIAL. The SIO, including those who are heads of elements
1198 of the IC and those designated according to paragraph 6.c of this enclosure, shall:

1199
1200 a. In accordance with Reference (b):

1201
1202 (1) Protect intelligence and intelligence sources and methods from unauthorized disclosure
1203 consistent with the policies of the DNI and, where applicable, the requirements of this Manual and
1204 Reference (j).

1205
1206 (2) Administer and oversee, within their respective organizations, those aspects of the SCI
1207 security programs not delegated to Defense Intelligence Agency (DIA) in accordance with
1208 Reference (b).

1209
1210 (3) Develop DoD Component-specific implementation guidance as necessary for the
1211 protection of SCI.

1212
1213 b. Cooperate and coordinate with the Component senior agency official as appropriate to
1214 achieve a harmonized and cohesive information security program within the DoD Component.

1215
1216 c. Where required by this Manual, provide the USD(I&S) with copies of requests for
1217 exceptions and waivers of information security policies, security incident reports, and other
1218 information submitted to the DNI.

1219
1220 d. Designate, as required by Intelligence Community Directive 703 (Reference (ad)) and
1221 Reference (j), an activity SSO to be responsible for the day-to-day security management, operation,
1222 implementation, use, and dissemination of SCI within the activity and, as needed, alternate SSO(s).
1223 Such designations shall be made for any activity that is accredited for and authorized to receive,
1224 use, and store SCI and shall be in writing.

1225
1226 (1) All SCI matters shall be referred to the SSO.

1227
1228 (2) The SSO may be designated as the activity security manager if the grade requirements
1229 for the position are met; however, the activity security manager cannot function as the SSO unless
1230 so designated by the cognizant senior intelligence official.

1231
1232
1233 12. INFORMATION SYSTEMS SECURITY OFFICIALS. ISSO (e.g., SAO, ISSM, and/or
1234 Information Systems Security Officer) designated, in writing, as required by DoDI 8500.01
1235 (Reference (ae)), shall:

1236
1237 a. Coordinate with the activity security manager regarding implementation of information
1238 systems security measures and procedures.

1239
1240 b. Notify the activity security manager, who retains overall security responsibility for required
1241 inquiries and investigations, when there are incidents involving possible or actual compromise or
1242 data spills of classified information resident in information systems, as required by Reference (ae),
1243 and coordinate with him or her, as required, for resolution of the incident.

...

ENCLOSURE 3DoD INFORMATION SECURITY PROGRAM OVERVIEW

- 1244
1245
1246
1247
1248
1249
1250 1. PURPOSE. Effective execution of a robust information security program that gives equal
1251 priority to both protecting information and demonstrating a commitment to open government and
1252 that includes accurate, accountable application of classification standards and routine, secure, and
1253 effective declassification is a national security imperative. This Manual provides overarching
1254 program guidance and direction for the DoD Information Security Program. While day-to-day
1255 program execution is the responsibility of all DoD personnel, program implementation must be
1256 guided by active and engaged senior managers at all levels who have the responsibility for overall
1257 program execution and by security managers who ensure the program is visible, effective, and
1258 efficient.
1259
1260
- 1261 2. SCOPE. The DoD Information Security Program implements References (b), (d), and (f) with
1262 regard to the classification, declassification, and protection of classified information, including
1263 information categorized as collateral, SCI, and SAP, and provides guidance to users to identify,
1264 mark, and protect certain types of unclassified information, referred to as CUI, in accordance with
1265 Reference (e), Reference (f), and other national-level directives. This combined guidance is known
1266 as the DoD Information Security Program and is applicable to all DoD Components.
1267
1268
- 1269 3. PERSONAL RESPONSIBILITY. All personnel of the DoD are personally and individually
1270 responsible for properly protecting classified information and CUI under their custody and control.
1271 All officials within the DoD who hold command, management, or supervisory positions have
1272 specific, non-delegable responsibility for the quality and effectiveness of implementation and
1273 management of the information security program within their areas of responsibility.
1274
1275
- 1276 4. NATIONAL AUTHORITIES FOR SECURITY MATTERS
1277
- 1278 a. President of the United States. The President of the U.S. bears executive responsibility for
1279 the security of the Nation, which includes the authority to classify information for the protection of
1280 the national defense and foreign relations of the U.S. The President has established standards for
1281 the classification, safeguarding, and declassification of national security information through the
1282 issuance of Reference (d) and for the designation and protection of CUI through the issuance of
1283 Reference (e).
1284
- 1285 b. National Security Council (NSC). In accordance with section 3021 of title 50, U.S.C.
1286 (Reference (af)), the NSC provides overall policy guidance on information security.

...

1287
1288 c. DNI. The DNI is head of the IC and principal advisor to the President and the NSC for
1289 intelligence matters related to national security pursuant to Section 1011 of Public Law 108-458
1290 (Reference (ag)) and Section 1.3 of E.O. 12333 (Reference (ah)). The DNI is also charged by
1291 section 1.3(b)(8) of Reference (ah) with protecting intelligence sources, methods, and activities,
1292 and in this role, the DNI issues instructions in the form of Intelligence Community Directives or
1293 other security policies and standards for the protection, management and oversight of SCI and other
1294 national intelligence.

1295
1296 d. ISOO. The ISOO, under the authority of the Archivist of the U.S., acting in consultation
1297 with the NSC, issues directives as necessary to implement Reference (d). The directives establish
1298 national standards for the classification and marking of national security information, security
1299 education and training programs, safeguarding, self-inspection programs, and declassification. The
1300 ISOO has the responsibility to oversee agency implementation and compliance with these
1301 directives. In this role, the ISOO requests certain information regarding DoD activities, and such
1302 requests are coordinated through USD(I&S).

1303
1304 e. CUI Office (CUIO). The CUIO, under the authority of the Archivist of the U.S., issues
1305 directives as necessary to implement Reference (e). The directives establish national standards for
1306 designation, safeguarding, marking, and dissemination of CUI as well as standards for education
1307 and training. The CUIO has the responsibility to oversee agency implementation and compliance
1308 with these directives. CUIO requests for information regarding DoD activities are coordinated
1309 through USD(I&S).

1310
1311 f. ***(Added)(DAF) SAF/AZ administers and oversees the DAF CUI program. The**
1312 **MAJCOM/FLDCOM, along with the local IP offices, serve as the CUI program managers**
1313 **and execute their respective programs, in accordance with DoDI 5200.48_DAFI 16-1403,**
1314 ***Controlled Unclassified Information (reference (bx)).***

1315
1316
1317 5. DoD INFORMATION SECURITY PROGRAM MANAGEMENT

1318
1319 a. USD(I&S). Reference (a) designates the USD(I&S) as the DoD Senior Security Official.
1320 In this role, the USD(I&S) is the DoD SAO responsible for directing, administering, and
1321 overseeing the DoD Information Security Program for the DoD, and except as provided in
1322 paragraph 5.b. of this section, performs the functions specified in subsection 5.4(d) of Reference (d)
1323 and its implementing directives for the DoD. The USD(I&S) is also the Restricted Data
1324 Management Official for the DoD consistent with the requirement in part 1045 of title 10, C.F.R.
1325 (References (ai) and (as)).

1326
1327 b. USD(P). In accordance with Reference (p), the USD(P) is the senior official responsible for
1328 directing, administering, and overseeing that portion of the DoD Information Security Program
1329 pertaining to foreign government (including NATO) information, the disclosure of classified
1330 information to foreign governments and international organizations, and security arrangements for
1331 international programs. Within the scope of these responsibilities, the USD(P) also performs the
1332 functions specified in subsection 5.4(d) of Reference (d) and its implementing directives for the
1333 DoD.

1334
1335 c. DoD CIO. In accordance with DoDD 5144.02 (Reference (aj)), the DoD CIO is responsible

1336 for all matters relating to the DoD information enterprise, including communications; spectrum
 1337 management; network policy and standards; information systems; cybersecurity; positioning,
 1338 navigation, and timing policy; and the DoD information enterprise that supports DoD command
 1339 and control.

1340
 1341 d. National Security Agency/Central Security Service (NSA/CSS). In accordance with
 1342 Reference (ah), the NSA/CSS provides centralized coordination and direction for signals
 1343 intelligence. In accordance with National Security Directive 42 (Reference (ak)), the NSA/CSS
 1344 provides IA/cybersecurity support for national security systems and, at the request of the national
 1345 security system owner, provides vulnerability assessments. Additionally, in accordance with
 1346 Reference (b), the Director, NSA/Chief, CSS may impose special requirements for protection of
 1347 classified cryptologic information.

1348
 1349 e. DIA. As assigned by Reference (b) and with the exception of NSA/CSS, the National
 1350 Reconnaissance Office, and the National Geospatial-Intelligence Agency, DIA administers within
 1351 the Department of Defense the SCI security policies and procedures issued by the DNI. The
 1352 Director, DIA, is responsible for development of standards, implementation, and operational
 1353 management of the SCI compartments for the DoD.

1354
 1355 f. Defense Counterintelligence and Security Agency (DCSA). DCSA provides information
 1356 security education and training for the DoD, as required by DoDI 3305.13 (Reference (al)). DCSA,
 1357 as the DoD cognizant security office for industrial security, also manages and administers the DoD
 1358 portion of the National Industrial Security Program, to ensure the protection of classified
 1359 information released or disclosed to industry in connection with classified contracts.

1360
 1361 g. DTIC. DTIC maintains a repository and index of security classification guides, as specified
 1362 in paragraph 6.c of Enclosure 6 of this Volume, for the DoD. DTIC also administers and controls
 1363 secondary release and dissemination of technical documents and data, including production,
 1364 engineering, and logistics information, marked with the distribution statements required by DoDI
 1365 5230.24 (Reference (am)). Such citations serve as the authoritative record for controlling office
 1366 classification and distribution decisions for the documents in the DTIC collections.

1367
 1368 h. **(Added)(DAF) The Commander, Headquarters United States Air Forces in Europe-**
 1369 **Air Forces Africa (USAFE-AFAFRICA) serves as the executive agent for the DAF NATO**
 1370 **program, representing the DAF at NATO meetings and interagency forums, and forwards**
 1371 **requests to establish and disestablish DAF sub-registries to the Central United States Registry**
 1372 **(CUSR).**

1373
 1374 i. ***(Added)(DAF) The Director, SAF/CN serves as the DAF CIO, in accordance with**
 1375 **SecAF Memorandum, *Delegation of Authority as Chief Information Officer under USC § 3506***
 1376 **(reference (by)), charged with carrying out DAF's responsibilities for information resources**
 1377 **management, information technology, and national security systems under 44 USC §3506 and**
 1378 **10 USC § 2223, as implemented by the Department of Defense.**

1381 6. DoD COMPONENT INFORMATION SECURITY MANAGEMENT

1382
 1383 a. Head of the DoD Component. The Head of each DoD Component has overall responsibility
 1384 for implementation of the information security program within the Component. This includes

1385 responsibility for:

1386
1387 (1) Designating SAO, including, as appropriate, the DoD Component SAO and SIO, to be
1388 responsible for directing, administering, and overseeing the information security program within
1389 the Component. A separate senior official responsible for overseeing SAPs, within the Component,
1390 may also be designated.

1391
1392 (2) Committing necessary resources to effectively implement the information security
1393 program.

1394
1395 b. SAO. The SAO has day-to-day responsibility for the direction, implementation, and
1396 oversight of Component's information security program and for its efficient and effective
1397 implementation. These responsibilities include:

1398
1399 (1) Promulgating guidance necessary for program implementation.

1400
1401 (2) Ensuring adequate resources for a robust information security program are identified
1402 and programmed.

1403
1404 (3) Establishing and maintaining a security education program.

1405
1406 (4) Establishing and maintaining an ongoing self-inspection and program oversight
1407 function.

1408
1409 (5) Directing the head of each activity within the DoD Component that creates, handles, or
1410 stores classified information to appoint an official to serve as security manager for the activity, to
1411 properly manage and oversee the activity's information security program.

1412
1413 c. Activity Security Management. The activity security manager manages and implements the
1414 activity's information security program and ensures its visibility and effectiveness on behalf of the
1415 activity head, who retains the responsibility for overall management and functioning of the
1416 program. The activity security manager must have sufficient delegated authority to ensure that
1417 personnel adhere to program requirements, and their position within the organizational hierarchy
1418 must ensure their credibility and enable them to raise security issues directly to their respective
1419 activity head.

1420
1421 (1) Some tasks may be assigned to a number of activity personnel and may even be
1422 assigned to persons senior to the security manager. Nevertheless, the activity security manager
1423 shall remain cognizant of all activity information, personnel, information systems, and physical and
1424 industrial security functions, and shall ensure that the information security program is coordinated
1425 and inclusive of all requirements in this Manual.

1426
1427 (2) Activity security manager responsibilities include:

1428
1429 (a) Serving as the principal advisor and representative to the activity head in all matters
1430 pertaining to this Manual.

1431
1432 (b) Developing a written activity security instruction.

...

1434 (c) Ensuring that personnel in the activity who perform security duties are trained.

1435
1436 (d) Formulating, coordinating, and conducting the activity security education training
1437 and awareness program.

1438
1439 d. TSCO. TSCOs are not required, but the activity head may elect to appoint a TSCO to
1440 facilitate appropriate control of top secret material when there is a need (e.g., accountability of
1441 Sigma 14 material as required in Volume 2 of this Manual). The TSCO maintains, for paper and
1442 other physical media (e.g., disk drives and removable computer media), a system of accountability
1443 (e.g., a registry) for activity top secret information and conducts inventories of Top Secret
1444 information.

1445
1446 (1) When collateral top secret information is maintained in a sensitive compartmented
1447 information facility (SCIF) or SAP-accredited facility, it may be handled in the same manner as
1448 SCI and SAP materials once necessary receipts have been provided to the organization supplying
1449 the materials. When collateral top secret material is taken out of a SCIF or SAP-accredited facility
1450 it shall be reentered into the registry system for accountability.

1451
1452 (2) Repositories, libraries, or activities that store large volumes of classified documents
1453 may limit their annual inventory to that which access has been given in the past twelve (12)
1454 months, and ten (10) percent of the remaining inventory.

1455
1456 (3) Accountability for Top Secret SCI, SAP, and other special types of classified
1457 information shall be in accordance with References (j) through (y), and other applicable guidance.

1458
1459 (4) ***(Added)(DAF) The establishment of a top secret control and accountability**
1460 **system is not mandatory. However, if the commander/director elects to appoint a TSCO to**
1461 **facilitate appropriate control of top secret material, procedures for the control and**
1462 **accountability must be developed. (T-1). These procedures must provide the means of**
1463 **facilitating oversight and management of top secret access controls, assessment and**
1464 **management of holdings, and identification of material at risk, in cases of potential**
1465 **unauthorized disclosure. In developing these procedures, the following requirements must be**
1466 **met, at minimum.**

1467
1468 (a) ***(Added)(DAF) The TSCO and one or more alternates will be designated, in**
1469 **writing. (T-1).**

1470
1471 (b) ***(Added)(DAF) The registry must include, at minimum, the title, date of**
1472 **creation, originator, copy number, and disposition. Top secret material will be numbered**
1473 **serially and marked to indicate its copy number, and accounted for. (T-1).**

1474
1475 (c) ***(Added)(DAF) Top secret material will be inventoried at least once annually,**
1476 **at minimum. (T-1). The inventory must reconcile the top secret accountability registry and**
1477 **records, with 100 percent of the top secret holdings. The inventory will be conducted by two,**
1478 **appropriately cleared personnel; the TSCO (or alternate) and a disinterested party that is not**
1479 **a TSCO, alternate, or subordinate within the chain of command. (T-1). The inventory will**
1480 **consist of a physical sighting of the material or written evidence of authorized disposition,**
1481 **such as certificate of destruction or receipt of transfer. (T-1).**

1482

1483 (d) ***(Added)(DAF) Before leaving the command, the TSCO (or alternate) will**
1484 **conduct a 100 percent inventory with the new TSCO of all top secret material in the registry.**
1485 **(T-1).**

1486
1487 e. Other Security Management Roles

1488
1489 (1) Assistant Security Manager. In large activities and where circumstances warrant,
1490 activities may designate U.S. Government civilian or military members as an assistant security
1491 manager, to assist the activity security manager with program implementation, maintenance, and
1492 local oversight.

1493
1494 (2) Security Assistants. As warranted, activities may assign U.S. Government civilian,
1495 military members, or contractor-support personnel as security assistants to perform administrative
1496 security functions under the direction of the activity security manager without regard for job series
1497 or title or for rank, rate, or grade as long as they have the clearance required for the access needed
1498 to perform their assigned duties and tasks (Note: While the scope of responsibilities and job titles
1499 covered by the General Schedule (GS) 0086 Security Clerical and Assistance Series can be
1500 consistent with the duties of a security assistant, as described in this paragraph, the role of security
1501 assistant does not require that civilian employees hold this job series).

1502
1503 (3) Communication Security (COMSEC) Custodian. The COMSEC Custodian is the
1504 activity head's primary advisor on matters concerning the security and handling of COMSEC
1505 information and hardware and the associated records and reports and functions in accordance with
1506 NSA/CSS Policy Manual 3-16 (Reference (an)).

1507
1508 (4) NATO Control Point Officer. In accordance with Reference (t), the Secretary of the
1509 Army operates the CUSR, the main receiving and dispatching element for NATO information in
1510 the U.S. Government. The activity NATO Control Point Officer, and any designated alternate(s),
1511 ensure that NATO information is correctly controlled and accounted for and that NATO security
1512 procedures specified in Reference (u) are followed. The CUSR manages the U.S. Registry system
1513 of sub-registries, communications centers, and control points to maintain accountability of NATO
1514 classified information and it conducts inspections of the associated security processes and
1515 procedures. Further information can be found at <http://www.cusr.army.mil>.

1516
1517 (5) SSO. An SSO is to be designated by the Senior Intelligence Official for any activity
1518 that is accredited for and authorized to receive, process, and store SCI. The activity SSO is
1519 responsible, in accordance with References (j) and (ad), for the day-to-day security management,
1520 operation, implementation, use, and dissemination of SCI within the activity.

1521
1522 (6) SAP Security Officer. In accordance with the requirements of Reference (q), a SAP
1523 security officer is to be designated for any activity that is accredited for and authorized to receive,
1524 use, and store SAP information.

1525
1526 (7) Information Systems Security Officials. Information systems security officials manage
1527 and oversee the DoD IT infrastructure (i.e., computer systems and networks). As computers are
1528 found everywhere within the DoD, close coordination with these officials regarding
1529 implementation of security measures and procedures is imperative.

1530
1531 (8) CI and OPSEC. The activity's information security program must also be closely

1532 coordinated and aligned with the DoD Component's CI and OPSEC functions in order to maintain
1533 the security essential to warfighter and mission success.

1534
1535 **(9) *(Added)(DAF) The Secretary of the Air Force, Chief Information Security**
1536 **Officer (SAF/CNZ) is charged with overseeing, developing and executing the DAF**
1537 **cybersecurity program (reference (by)).**

1538
1539
1540 **7. USE OF CONTRACTORS IN SECURITY ADMINISTRATION.** In accordance with DoDI
1541 1100.22 (Reference (ao)) and Office of Federal Procurement Policy Letter 11-01 (Reference (ap)),
1542 there are certain critical, closely associated with inherently governmental, or otherwise exempt
1543 functions and activities that cannot or should not be performed by a contractor. The DoD
1544 Components shall be careful not to outsource security functions that are inherently governmental.

1545
1546 a. Activity security management shall ensure that contractors who are involved in security
1547 administration and support duties are clearly identified in their capacities, roles, and functions, to
1548 ensure there is no possible confusion regarding which security personnel may exercise inherently
1549 governmental authorities and which may not.

1550
1551 b. Inherently governmental activities and functions include those that require either the
1552 exercise of substantial discretion in applying U.S. Government authority, or value judgments when
1553 making decisions for the U.S. Government. Inherently governmental security functions include,
1554 but are not limited to:

1555
1556 (1) Approving and issuing security policies and procedures.

1557
1558 (2) Making original classification decisions, or rendering classification determinations
1559 regarding classified information that is improperly or incompletely marked (Note: Correcting
1560 improper markings when the appropriate classification is not in question is not considered
1561 rendering a classification determination).

1562
1563 (3) Deciding to downgrade or declassify information (Note: Adhering to security markings
1564 on information or to guidance stated in an appropriate security classification or declassification
1565 guide is not considered a downgrading or declassification decision).

1566
1567 (4) Deciding challenges to classification and any appeals.

1568
1569 (5) Making foreign disclosure decisions pursuant to Reference (y).

1570
1571 (6) Making public release decisions pursuant to Reference (v).

1572
1573 (7) Committing to expenditure of U.S. Government funds pursuant to References (ao) and
1574 (ap).

1575
1576 (8) Conducting investigations of, or determining fault in, security incidents involving U.S.
1577 Government or other contractor personnel (Note: Contractors may conduct preliminary inquiries to
1578 determine if a security incident is a violation or an infraction).

1579
1580 (9) Giving final approval or executing documents for filing in litigation if documents assert

1581 an official position of the DoD, any DoD Component, or any other Federal agency.

1582
1583
1584 8. USE OF FOREIGN NATIONALS IN SECURITY ADMINISTRATION. Foreign nationals
1585 may not engage in the following DoD security administrative activities:

1586 a. Approving and issuing security policies and procedures

1587
1588 b. Making original classification decisions, or rendering classification determinations
1589 regarding classified information that is improperly or incompletely marked (Note: Correcting
1590 improper markings when the appropriate classification is not in question is not considered
1591 rendering a classification determination).

1592
1593 c. Deciding to downgrade or declassify information (Note: Adhering to security markings on
1594 information or guidance stated in an appropriate security classification or declassification guide is
1595 not considered a downgrading or declassification decision).

1596
1597 d. Deciding challenges to classification or any appeals.

1598
1599 e. Making foreign disclosure decisions pursuant to Reference (y).

1600
1601 f. Making public release decisions pursuant to Reference (v).

1602
1603 g. Committing to expenditure of U.S. Government funds; guidelines within international or
1604 host nation agreements or treaties may provide exceptions to this area of security administration.

1605
1606 h. Conducting investigations of, or determining fault in, security incidents involving U.S.
1607 Government or contractor personnel.

1608
1609 i. Giving final approval or executing documents for filing in litigation, if documents assert an
1610 official position of the DoD, any DoD Component, or any other federal agency.

1611
1612 j. Escorting personnel, except where the foreign national is employed by DoD and the foreign
1613 national escorts personnel:

1614
1615 (1) As a specific function of his or her assigned duties.

1616
1617 (2) Only to areas where U.S. personnel are embedded within locations or facilities that are
1618 outside the continental U.S.

1619
1620 (3) Only in situations not detrimental to the interests of the DoD or the U.S. Government.

1621
1622 k. Accessing combinations at the entrance and exit doors or security containers that contain
1623 non-releasable classified information or non-releasable CUI.

1624
1625 l. Accessing codes or functions associated with the intrusion detection system or master codes
1626 associated with access control devices.

1627
1628 m. Accessing IT equipment, such as computers, printers, or fax equipment used to process
1629

...

1630 non-releasable classified information or non-releasable CUI.

1631
1632 n. Constructing or modifying areas where classified information will be processed, unless
1633 cleared U.S. national civil engineers provide oversight to all new construction and modifications of
1634 facilities where classified information will be processed.

1635
1636 o. Accessing SCIFs, except as stated in Volume 2 of Reference (j).

1637
1638
1639 9. CLASSIFICATION AUTHORITY. Except for information subject to section 2011 et seq., of
1640 title 42, U.S.C. (also known and hereinafter referred to as “The Atomic Energy Act of 1954, as
1641 amended” (Reference (aq))), Reference (d) and this Manual provide the only authority for
1642 applying security classification to information within the DoD.

1643
1644
1645 10. CLASSIFICATION POLICY. Information shall be classified only when necessary in the
1646 interests of national security and shall be declassified as soon as is consistent with the
1647 requirements of national security.

1648
1649
1650 11. RECLASSIFICATION. After information has been declassified and released to the public
1651 under proper authority, it may be reclassified only in accordance with paragraph 17.b. of
1652 Enclosure 4.

1653
1654
1655 12. ACCESS TO CLASSIFIED INFORMATION

1656
1657 a. Requirements for Access. Persons shall be allowed access to classified information only if
1658 they:

1659
1660 (1) Possess current security clearance eligibility, in accordance with Reference (s).

1661 Reference (s) contains detailed guidance on personnel security investigations, adjudications, and
1662 accesses;

1663
1664 (2) Have executed an appropriate non-disclosure agreement; and

1665
1666 (3) Have a valid need-to-know for the information, in order to perform a lawful and
1667 authorized governmental function.

1668
1669 b. Nondisclosure Agreements

1670
1671 (1) Before being granted access to confidential, secret, or top secret information, employees
1672 shall sign the SF 312, “*Classified Information Nondisclosure Agreement*,” or other non-disclosure
1673 agreement approved by the DNI. SF 312 (or its predecessor, SF 189), or a legally enforceable
1674 facsimile retained in lieu of the original, shall be maintained for 50 years from the date of signature.
1675 Electronic signatures shall not be used to execute the SF 312.

1676
1677 (2) Before being granted access to SCI information, individuals adjudicated and approved
1678 for access shall sign a DNI-authorized SCI nondisclosure agreement. Consistent with the

...

1679 provisions of DoDD 5210.48 (Reference (ar)) and all applicable laws, that agreement shall include,
1680 as an addendum, the individual's written certification that they may be asked to undergo a
1681 polygraph examination in connection with any investigation of an unauthorized disclosure of SCI
1682 information to which they have had access.

1683
1684 (3) Before being granted access to SAP information, individuals adjudicated and approved
1685 for access shall additionally sign a DoD-approved program indoctrination agreement(s) for that
1686 information as required by Reference (q). Before gaining access and during a period of access to
1687 DoD SAPs, all personnel shall consent to, and be subject to, a random CI-scope polygraph
1688 examination, as required by Reference (q).

1689
1690 c. NATO Briefing for Cleared Personnel. To facilitate potential access to NATO classified
1691 information, all DoD military and civilian personnel who are briefed on their responsibilities for
1692 protecting U.S. classified information shall be briefed simultaneously on the requirements for
1693 protecting NATO information. A written acknowledgement of the individual's receipt of the
1694 NATO briefing and responsibilities for safeguarding NATO classified information shall be
1695 maintained. As stipulated in Reference (u), access to NATO classified information shall also
1696 require a supervisor's determination of the individual's need to know and possession of the
1697 requisite security clearance. Receipt of the NATO briefing shall be verified prior to granting access
1698 to NATO classified information.

1699
1700 d. Access by Individuals outside the Executive Branch. See section 6, Enclosure 2 of Volume
1701 3 of this Manual for further guidance regarding access to classified information by individuals
1702 outside the Executive Branch.

1703
1704
1705 13. PROTECTION REQUIREMENTS. Classified information and CUI shall be protected at all
1706 times. Volumes 1 through 3 of this Manual provide guidance for the protection of classified
1707 information, while DoDI 5200.48 provides guidance for the protection of CUI. Additional
1708 guidance for special types of information is provided by this section.

1709
1710 a. Protection of Restricted Data (RD) and Formerly Restricted Data (FRD). Classified
1711 information, including Critical Nuclear Weapon Design Information (CNWDI), in the custody of
1712 the DoD and marked as RD or FRD in accordance with the Atomic Energy Act of 1954, as
1713 amended, shall be stored, protected, and destroyed as this Manual requires for other information of
1714 a comparable level of security classification.

1715
1716 (1) Consult DoDI 5210.02 (Reference (as)) for DoD policy and procedures concerning
1717 access to and dissemination of RD, FRD and CNWDI, within the DoD. Reference (as) also
1718 provides guidance on access, distribution, handling, and accountability of Sigma information.

1719
1720 (2) Until DoD public key infrastructure is generally deployed on the Secret Internet
1721 Protocol Router Network (SIPRNET), the following security measures, deemed sufficient to
1722 provide the access and dissemination controls, required by Reference (as), shall be implemented
1723 when processing RD and CNWDI on SIPRNET:

1724
1725 (a) RD and CNWDI shall be emailed only after confirmation that the recipient has
1726 security clearance eligibility and access, at the appropriate level, has a need-to-know for the
1727 information, and, for CNWDI, has received the additional security briefing required by Reference

...

1728 (as).

1729

1730 (b) All RD and CNWDI files stored on shared or personal local electronic storage
1731 devices shall be password-protected.

1732

1733 (c) IT systems and networks must be certified and accredited for RD, FRD, and/or
1734 CNWDI prior to transmission, processing, or storage of such data. Such certification must verify
1735 that access to RD, FRD, and CNWDI information, including through websites, is limited to
1736 authorized recipients by, at a minimum, a properly administered and protected individual identifier
1737 and password consistent with requirements of Reference (ae).

1738

1739 (d) System logons and properly configured screen savers are sufficient protection for
1740 e-mail files.

1741

1742 (e) In accordance with Reference (as), Sigma 14, 15, and 20 information shall not be
1743 processed on SIPRNET.

1744

1745 b. Protection of SCI. SCI information shall be controlled and protected in accordance with
1746 applicable national policy, policies established by the DNI, and implementing DoD issuances.
1747 Security classification and declassification policies of this Manual apply to SCI information in the
1748 same manner as other classified information.

1749

1750 c. Protection of COMSEC Information. COMSEC information shall be controlled and
1751 protected in accordance with applicable national policy and DoD issuances. Security classification
1752 and declassification policies of this Manual apply to COMSEC information in the same manner as
1753 other classified information, except ONLY NSA/CSS is authorized to declassify COMSEC
1754 information.

1755

1756 d. Protection of SAP Information. SAPs shall be created, continued, managed, and
1757 discontinued in accordance with Reference (q) and DoDI 5205.11 (Reference (at)). Information
1758 covered by SAPs established in accordance with References (q) and (at) shall be classified,
1759 declassified, controlled, and protected as this Manual, References (q) and (at), and instructions
1760 issued by officials charged with management of those programs require. The provisions of this
1761 Manual pertaining to classification, declassification, and marking apply, without exception, to SAP
1762 information unless waivers of specific requirements are obtained in accordance with section 16 of
1763 this enclosure.

1764

1765 e. Protection of NATO and FGI. NATO classified information shall be safeguarded consistent
1766 with References (d) and (u). Other FGI shall be safeguarded consistent with Reference (d) and the
1767 requirements of this Manual, except as required by the Appendix to Enclosure 4 of Volume 3;
1768 treaties; or international agreements. Information that is jointly developed with a foreign partner
1769 under a cooperative program agreement will be safeguarded in accordance with the security and
1770 disclosure provisions of the cooperative arrangement.

1771

1772 f. Protection of Nuclear Command and Control-Extremely Sensitive Information (NC2-ESI).
1773 Certain information pertaining to the command and control of nuclear weapons is designated NC2-
1774 ESI. NC2-ESI information shall be marked, safeguarded, and distributed in accordance with
1775 Chairman of the Joint Chief of Staff Instruction 3231.01B (Reference (au)).

1776

...

1777
1778 14. RETENTION. Classified information and CUI shall be maintained only when it is required for
1779 effective and efficient operation of the organization or if law, treaty, international agreement, or
1780 regulation requires its retention. Such information shall be disposed in accordance with the
1781 provisions of chapter 33 of title 44, U.S.C. (Reference (av)), as implemented by DoDD 5015.02
1782 (Reference (aw)), and DoD Component implementing directives and records schedules.

1783
1784
1785 15. PERMANENTLY VALUABLE RECORDS. Classified and CUI documents and material that
1786 constitute permanently valuable records of the U.S. Government shall be maintained and disposed
1787 of in accordance with Reference (aw) and appropriate DoD Component directives and records
1788 schedules. Other classified and CUI material shall be destroyed as specified in this Manual. When
1789 transferring classified records for storage or archival purposes to the National Archives and
1790 Records Administration (NARA) or to other locations, identify the boxes that contain foreign
1791 government documents as well as DoD documents containing FGI.

1792
1793
1794 16. MILITARY OPERATIONS. Military commanders may modify the provisions of this Manual
1795 pertaining to accountability, dissemination, transmission, and storage of classified and CUI material
1796 and information as necessary to meet local conditions encountered during military operations.
1797 Military operations include combat and peacekeeping operations but not routine Military
1798 deployments or exercises. Classified information and CUI shall be introduced into combat areas or
1799 zones, or areas of potential hostile activity, only as necessary to accomplish the military mission.

1800
1801
1802 17. WAIVERS AND EXCEPTIONS. Unless otherwise specified in this Volume, the DoD
1803 Components must submit requests for information security waivers or exceptions to the standards
1804 and requirements in this Manual through the chain of command to the USD(I&S), Attn: Director,
1805 Security Policy and Oversight Division, for approval.

1806
1807 a. If the waiver or exception involves any of the other security areas (e.g., industrial, physical,
1808 personnel), it must first be internally coordinated with the applicable security office(s) before the waiver
1809 or exception request is submitted for endorsement by the SAO. This may involve a separate request for
1810 waiver or exception based on the requirements of the other security policy issuances.

1811
1812 b. Waivers or exceptions pertaining to foreign government (including NATO) information and
1813 security arrangements for international programs must only be submitted to and approved by the
1814 USD(P), who will ensure concurrence by the USD(I&S) if the request involves the any of the
1815 security disciplines.

1816
1817 c. The Military Departments will forward requests for waiver or exception through their SAOs
1818 for endorsement before submitting such requests to the USD(I&S) for approval. DoD Components
1819 will provide all requests for waiver or exception, including those approved by the USD(P), to the
1820 USD(I&S) through the Director, Security Policy and Oversight Division. The USD(I&S) and
1821 USD(P) shall be responsible for promptly notifying the Director, ISOO, of approved waivers and
1822 exceptions involving References (d) and (f).

1823
1824 d. Requests for information security waivers and exceptions shall contain sufficient
1825 information to permit a complete and thorough analysis to be made of the impact of approval on

...

1826 National Security. Minimally, requests must identify the specific provision(s) of this Manual for
1827 which the waiver or exception is sought (cite this Manual by volume, enclosure, and paragraph)
1828 and provide rationale and justification for the request, including negative impacts to cost, schedule,
1829 mission, or operations; a mission analysis summary to identify vulnerabilities and risk management
1830 considerations; a summary of proposed mitigation measures to reduce risk; and the necessary
1831 duration for any waivers. A sample template memorandum for requesting waivers and exceptions
1832 is at the Appendix to this enclosure. Current waivers and exceptions will continue to be valid until
1833 they are due for renewal.

1834
1835 e. In the case of information security waivers and exceptions involving classified information,
1836 the DoD Components shall maintain documents regarding approved waivers and exceptions, and
1837 furnish such documents to other agencies with which they share affected classified information or
1838 secure facilities, except documentation regarding approved waivers and exceptions involving
1839 marking of classified information need be shared only upon request.

1840 1841 1842 18. CORRECTIVE ACTIONS AND SANCTIONS

1843
1844 a. Procedures. Heads of the DoD Components shall establish procedures to ensure that prompt
1845 and appropriate management action is taken in cases of compromise of classified information and
1846 unauthorized disclosure of CUI, improper classification or designation of information, violation of
1847 the provisions of this Manual, and incidents that may put classified information and CUI at risk of
1848 unauthorized disclosure. Such actions shall focus on correcting or eliminating the conditions that
1849 caused or brought about the incident.

1850 1851 b. Sanctions

1852
1853 (1) DoD military and civilian personnel may be subject to criminal or administrative
1854 sanctions if they knowingly, willfully, or negligently:

1855
1856 (a) Disclose classified information to unauthorized persons.

1857
1858 (b) Classify or continue the classification of information in violation of this Volume.

1859
1860 (c) Create or continue a SAP contrary to the requirements of Reference (q) and this
1861 Volume.

1862
1863 (d) Disclose CUI to unauthorized persons.

1864
1865 (e) Violate any other provision of this Manual.

1866
1867 (2) Sanctions include, but are not limited to, warning, reprimand, suspension without pay,
1868 forfeiture of pay, removal, discharge, loss, or denial of access to classified information and/or CUI,
1869 and removal of classification authority. Criminal sanctions may also be undertaken in accordance
1870 with sections 801-940 of title 10, U.S.C. (also known as "The Uniform Code of Military Justice"
1871 (UCMJ) (Reference (ax))) and other applicable U.S. criminal laws.

1872
1873 (3) If an OCA demonstrates reckless disregard or a pattern of error in applying the
1874 classification standards of this Volume, the appropriate official shall, as a minimum, remove the

...

1875 offending individual's OCA.

1876

1877 c. Reporting of Incidents. Security incidents involving classified information shall be reported
1878 as required in Enclosure 6 of Volume 3 of this Manual. Incidents involving CUI shall be reported
1879 per DoDI 5200.48 requirements.

...

APPENDIX TO ENCLOSURE 3

DOD COMPONENT REQUEST FOR WAIVER OR EXCEPTION

[CLASSIFICATION]

COMPONENT SENIOR AGENCY OFFICIAL LETTERHEAD

[month, day, year]

MEMORANDUM FOR DIRECTOR, SECURITY POLICY AND OVERSIGHT DIVISION,
OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND
SECURITY

SUBJECT: Request for [Organization Name] Waiver [or Exception] (Information Security) from
DoDM 5200.01 Standard [or Requirement]

Purpose: The [Title, Organization Name] requests a waiver or exception from DoDM 5200.01,
[volume, enclosure, paragraph/section], for a [short description of the requirement or standard for
which the waiver or exception is sought]. [SAO title, Organization, Name] has reviewed this
request with attachments and concurs with this request.

Justification: [Brief description of the rationale and justification for the request for waiver
or exception, to include negative impacts to cost, schedule, mission, or operations.]

Mission Analysis Summary: A mission analysis that discusses missions and functions
impacted by this waiver or exception is at TAB A.

Risk Assessment: The risk management assessment at TAB B identifies vulnerabilities and
risk management considerations related to this request for waiver or exception.

Mitigation Measures: The mitigation measures at TAB C describe measures identified to
reduce risks identified at TAB B. [If there are no mitigation measures, state "None."] The [SAO
Title, Organization Title] concurs with this request and the mitigation measures and accepts the risk
level based on the mitigation measures to be taken.

Timeframe: This is a temporary waiver request from [start date] through [end date]; or, this
is a permanent exception request.

The POC for this action is [Name, Title, Organization, Phone number, email address].

[Signature Block of Component SAO]

Attachments:
As stated

[CLASSIFICATION]

ENCLOSURE 4CLASSIFYING INFORMATION1. CLASSIFICATION POLICY

a. Information shall be classified only to protect national security. If there is significant doubt about the need to classify information, it shall not be classified. Unnecessary or higher than necessary classification is prohibited by Reference (d). Information will be declassified as soon as it no longer qualifies for classification.

b. Classification may be applied only to information that is owned by, produced by or for, or is under the control of the U.S. Government. Information may be considered for classification only if its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security and it concerns one of the categories specified in section 1.4 of Reference (d):

- (1) Military plans, weapon systems, or operations (subsection 1.4(a));
- (2) FGI (subsection 1.4(b));
- (3) Intelligence activities (including covert action), intelligence sources or methods, or cryptology (subsection 1.4(c));
- (4) Foreign relations or foreign activities of the United States, including confidential sources (subsection 1.4(d));
- (5) Scientific, technological, or economic matters relating to the national security (subsection 1.4(e));
- (6) U.S. Government programs for safeguarding nuclear materials or facilities (subsection 1.4(f));
- (7) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security (subsection 1.4(g)); or
- (8) The development, production, or use of weapons of mass destruction (subsection 1.4(h)).

c. Information assigned a level of classification under Reference (d) or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings.

2. CLASSIFICATION PROHIBITIONS

a. Information may not be classified, continued to be maintained as classified, or fail to be declassified in order to:

...

1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019

- (1) Conceal violations of law, inefficiency, or administrative error.
- (2) Prevent embarrassment to a person, organization, or agency.
- (3) Restrain competition.

(4) Prevent or delay the release of information that does not require protection in the interests of the national security.

b. Basic scientific research and its results may not be classified unless clearly related to the national security.

3. LEVELS OF CLASSIFICATION. Information identified as requiring protection against unauthorized disclosure in the interest of national security shall be classified top secret, secret, or confidential. Except as otherwise provided by statute, no other terms shall be used to identify U.S. classified information.

a. Top Secret. Top secret shall be 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.

b. Secret. Secret shall be 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.

c. Confidential. Confidential shall be 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.

4. ORIGINAL CLASSIFICATION

a. Original classification is the initial decision that an item of information could reasonably be expected to cause identifiable or describable damage to the national security if subjected to unauthorized disclosure and requires protection in the interest of national security.

b. Information may be originally classified only by the Secretary of Defense, the Secretaries of the Military Departments, and other officials to whom they delegate this authority in writing. Delegation of OCA shall be limited to the minimum number of officials required for effective operation of the Department of Defense. The authority shall be delegated to, and retained by

only those officials who have a demonstrable and continuing need to exercise it. Component senior officials responsible for designating Component OCAs will annually review OCA positions to ensure all designated OCA positions are required.

c. Authority to classify information at any lower level of classification is inherent in delegation of OCA.

(1) Top Secret OCA. Information may be originally classified top secret only by the Secretary of Defense, the Secretaries of the Military Departments, or those officials to whom the Secretary of Defense or the Secretaries of the Military Departments have delegated this authority in writing.

(2) Secret and Confidential OCA. Information may be originally classified secret or confidential only by the Secretary of Defense, the Secretaries of the Military Departments, and those officials to whom such authority has been delegated in writing by the Secretary of Defense, the Secretaries of the Military Departments, or the senior agency officials of the Military Departments or Department of Defense appointed in accordance with section 5.4(d) of Reference (d), provided those senior agency officials have also been delegated top secret OCA.

d. The OCA for FGI is the foreign government originating the information.

5. REQUESTS FOR OCA

a. Requests for OCA for officials serving in the OSD and the DoD Components, other than the Military Departments, including the Office of the Chairman of the Joint Chiefs of Staff, the Joint Staff, and the Combatant Commands, shall be submitted to the USD(I&S) for approval. These requests shall specify the position title for which the authority is requested, provide a brief, mission-specific justification for the request, and be submitted through established organizational channels. Heads of DoD Components, excluding the Military Departments, delegated Top Secret OCA are not authorized to delegate Secret and Confidential classification authority to subordinate officials.

(1) *(Added)(DAF) Requests for OCA delegation must be submitted through the MAJCOM/FLDCOM IP office to SAF/AAZ. (T-0). Requests will include, at minimum, the position title and a brief, mission-specific justification that supports a demonstrable and continuing need to exercise OCA, which cannot be met through the existing chain of command. (T-0).

(a) (Added)(DAF) Only the SecAF can delegate top secret OCA.

(b) (Added)(DAF) SAF/AA can delegate secret and confidential OCA.

(2) *(Added)(DAF) SAF/AAZ will maintain a consolidated list of DAF OCA delegations and make it available on its SharePoint® site.

(a) (Added)(DAF) On an annual basis, SAF/AAZ requests the MAJCOM/FLDCOMs, in coordination with the servicing IP offices, work with the OCAs to validate that each OCA still has a demonstrable and continuing need for the delegation. If

2069 **the need no longer exists, submit a voluntary withdrawal memo to SAF/AAZ.**

2070
2071 **(b) *(Added)(DAF) Biennially, SAF/AAZ will route the OCA listing to SecAF for**
2072 **endorsement. During revalidation, SAF/AAZ will request the SecAF rescind OCA, when a**
2073 **demonstrable need is not being met.**

2074
2075 b. Requests for OCA shall be approved only when:

2076
2077 (1) There is a demonstrable and continuing need to exercise OCA during the normal
2078 course of operations (As a general rule, absent issuance of a security classification guide, an OCA
2079 must exercise this authority an average of twice a year to justify and retain designation as an OCA).

2080
2081 (2) Such demonstrable and continuing need cannot be met through issuance of security
2082 classification guides by existing OCAs in the chain of command.

2083
2084 (3) Referral of decisions to existing OCAs at higher levels in the chain of command or
2085 supervision is not practical for reasons such as geographical separation.

2086
2087 (4) Sufficient expertise and information is available to the prospective OCA to permit
2088 effective classification decision-making.

2089
2090 c. OCA is designated by virtue of position. Each OCA delegation shall be in writing and the
2091 authority shall not be re-delegated except as provided in paragraph 4.c. of this enclosure. Each
2092 delegation shall identify the official to whom authority is delegated by position title. The Director
2093 of Security, USD(I&S), shall be notified in writing of all OCA delegations.

2094
2095 (1) Only senior positions (typically general and/or flag officer or Senior Executive Service
2096 or equivalent level) assigned a unique mission with responsibility in one of the subject areas cited
2097 in paragraph 1.b. of this enclosure may be designated an OCA.

2098
2099 (2) Deputies, vice commanders, chiefs of staff, and similar immediate subordinates of an
2100 OCA are empowered to exercise the OCA when they have been officially designated to assume the
2101 duty position of the OCA in an "acting" capacity during the OCA's absence and have certified in
2102 writing that they have received the OCA training required by Enclosure 5 of Volume 3 of this
2103 Manual.

2104
2105 d. Before exercise of the authority and annually thereafter, persons in positions with delegated
2106 OCA must certify, in writing, that they have received training in the fundamentals of proper
2107 security classification and declassification, the limitations of their authority, the sanctions that may
2108 be imposed, and OCA duties and responsibilities, as required by Enclosure 5 of Volume 3 of this
2109 Manual.

2110
2111 e. Activity security managers must ensure that OCA delegation letters and OCA training
2112 certifications are maintained and can be retrieved by the office assigned that responsibility when
2113 requested by appropriate authorities.

2114
2115
2116 6. ORIGINAL CLASSIFICATION PROCESS. All DoD OCAs are responsible to the Secretary
2117 of Defense for their classification decisions. In making a decision to originally classify

...

2118 information, they shall:

2119

2120 a. Determine that the information is owned by, produced by or for, or is under the control of
2121 the U.S. Government.

2122

2123 b. Determine the information falls within one or more of the categories of information listed in
2124 paragraph 1.b. of this enclosure.

2125

2126 c. Determine the information has not already been classified by another OCA.

2127

2128 d. Determine that classification guidance is not already available in the form of security
2129 classification guides, plans, or other memorandums. Within the DoD, the majority of existing
2130 classification guidance is indexed and promulgated via the DTIC, available at www.dtic.mil.

2131

2132 e. Determine that there is a reasonable possibility that the information can be provided
2133 protection from unauthorized disclosure. OCAs shall balance the cost to protect the information
2134 against the risks associated with its disclosure. The advantages must outweigh the disadvantages of
2135 classification.

2136

2137 f. Determine and assign the appropriate level of classification (i.e., top secret, secret, or
2138 confidential) to be applied to the information, based on reasoned judgment as to the degree of
2139 damage, which the OCA can describe, that could be caused by unauthorized disclosure. If there is
2140 significant doubt about the appropriate level of classification, it shall be classified at the lower
2141 level.

2142

2143 (1) Determine the probable operational, technological, and resource impact of
2144 classification.

2145

2146 (2) If decisions must be rendered verbally due to exigencies of an ongoing operation or
2147 other emergency, issue written confirmation within 7 calendar days of the decision and provide the
2148 required declassification and marking instructions.

2149

2150 (3) Be prepared to present, as required, depositions and expert testimony in courts of law
2151 concerning classification of national security information and to justify their original decisions.

2152

2153 (4) Be prepared to produce a written description of the damage, as necessary, for a
2154 classification challenge, a security classification review, a damage assessment, a request for
2155 mandatory review for declassification, a request for release under section 552 of title 5, U.S.C.
2156 (also known and hereinafter referred to as "The Freedom of Information Act" (Reference (ay))),
2157 when pertinent to judicial proceedings, or as other statute or regulation may require.

2158

2159 g. Determine the appropriate duration of classification to be applied to the information.
2160 Section 13 of this enclosure discusses the specific options available in making this decision.

2161

2162 h. Document the classification decision and clearly and concisely communicate it in writing
2163 to persons who shall possess the information by issuing classification guidance or by ensuring
2164 documents containing the information are properly marked to reflect the decision. Classification
2165 guidance may be communicated by issuance of a security classification or declassification guide or
2166 in the form of a memorandum, plan, order, or letter. If issued by other than a classification or

...

2167 declassification guide, the guidance should be incorporated in a guide in a timely fashion.
 2168 Enclosure 6 of this Volume discusses classification guides; Volume 2 of this Manual provides
 2169 marking guidance.

2170
 2171

2172 7. CHANGING THE LEVEL OF CLASSIFICATION

2173

2174 a. OCAs may change the level of classification of information under their jurisdiction,
 2175 provided the information continues to meet the standards for classification identified in this
 2176 enclosure. Documents shall be re-marked with the new classification level, the date of the action,
 2177 and the authority for the change. Changing the classification level may also require changing
 2178 portion markings for information contained within the document. Additionally, the OCA shall
 2179 update appropriate security classification guides and immediately notify all known holders of the
 2180 information of the changes. Sections 18 and 19 of Enclosure 5 of this Volume provide additional
 2181 guidance on downgrading and upgrading classified information.

2182
 2183

2184 8. SECURITY CLASSIFICATION GUIDANCE

2185

2186 a. The responsible OCA shall issue security classification guidance for each system, plan,
 2187 program, project, or mission involving classified information. Classification guidance may be in
 2188 the form of a memorandum, plan, order, letter, or issuance of a security classification or
 2189 declassification guide.

2190

2191 b. OCAs shall develop, as appropriate, automatic and systematic declassification guidance for
 2192 use in review of records that are of permanent historical value and 25 years old or older. This
 2193 guidance shall be published in the appropriate classification or declassification guide. FGI is
 2194 exempt from automatic declassification pursuant to paragraphs 3.3b (6) and 3.3f of Reference (d).

2195

2196 c. Exemptions from automatic declassification approved pursuant to section 13 of Enclosure 5
 2197 of this Volume may be incorporated into classification guides provided the ISCAP is notified of the
 2198 intent to take such action in advance and the information remains in active use. See paragraph 13.c.
 2199 of Enclosure 5 of this Volume for the notification process.

2200

2201 d. Where classification guidance is issued in the form of a security classification guide, the
 2202 OCA shall ensure the guide is reviewed and updated as specified in Enclosure 6 of this Volume.

2203

2204 e. As a general rule, classification authority must be exercised an average of twice a year to
 2205 qualify for retention of the OCA designation if an OCA does not issue and maintain a security
 2206 classification guide.

2207

2208 **f. (Added)(DAF) Security classification guidance containing RD, FRD, CNWDI, DOE**
 2209 **Sigma, or TFNI must be coordinated with AF/A10, prior to issuance and promulgation.**

2210

2211

2212 9. TENTATIVE CLASSIFICATION. Individuals who submit information to OCAs for original
 2213 classification decisions shall provide the OCA the information required by paragraphs 6.a. through
 2214 6.f. of this enclosure, and may, as necessary, tentatively classify information or documents as
 2215 working papers, pending approval by the OCA. Final classification decisions must be made as soon

...

as possible, but not later than 180 days from the initial drafting date of the document. Prior to the OCA's classification decision, such information shall be safeguarded as required for the specified level of classification and it shall not be used as a source for derivative classification.

10. DERIVATIVE CLASSIFICATION

a. When incorporating, paraphrasing, restating, or generating classified information in a new form or document (i.e., derivatively classifying information), it must be identified as classified information by marking or similar means. Derivative classification includes classification of information based on classification guidance in a security classification guide or other source material, but does not include photocopying or otherwise mechanically or electronically reproducing classified material.

b. Within the DoD all cleared personnel, who generate or create material that is to be derivatively classified, shall ensure that the derivative classification is accomplished in accordance with this enclosure. No specific, individual delegation of authority is required. DoD officials who sign or approve derivatively classified documents have principal responsibility for the quality of the derivative classification.

c. All persons performing derivative classification shall receive training, as specified in Enclosure 5 of Volume 3 of this Manual, on proper procedures for making classification determinations and properly marking derivatively classified documents.

d. *(Added)(DAF) All DAF personnel that process classified correspondence or utilize classified information systems are considered derivative classifiers. Derivative classifiers are responsible for applying the prescribed classification markings, controls and declassification instructions associated with the documents they create. Those who do so improperly, may be subject to sanctions identified in enclosure 3 of this volume. This includes maintaining a copy of the most current version of SCG being utilized to perform day-to-day duties.

11. RESPONSIBILITIES OF DERIVATIVE CLASSIFIERS. Derivative classifiers shall:

a. Observe and respect the classification determinations made by OCAs. If derivative classifiers believe information to be improperly classified, they shall take the actions required by section 22 of this enclosure.

b. Identify themselves and the classified information by marking it in accordance with Volume 2 of this Manual.

c. Use only authorized sources for classification guidance (e.g., security classification guides, memorandums, DoD publications, and other forms of classification guidance issued by the OCA) and markings on source documents from which the information is extracted for guidance on classification of the information in question. The use of memory alone or "general rules" about the classification of broad classes of information is prohibited.

d. Use caution when paraphrasing or restating information extracted from a classified source

document. Paraphrasing or restating information may change the need for or level of classification.

e. Take appropriate and reasonable steps, including consulting a security classification guide or requesting assistance from the appropriate OCA, to resolve doubts or apparent conflicts about the classification, level of classification, and duration of classification. In cases of apparent conflict between a security classification guide and a classified source document regarding a discrete item of information, the instructions in the security classification guide shall take precedence. Where required markings are missing or omitted from source documents, consult the OCA, appropriate security classification guide, or other classification guidance for application of the omitted markings.

12. PROCEDURES FOR DERIVATIVE CLASSIFICATION

a. Derivative classifiers shall carefully analyze the material they are classifying to determine what information it contains or reveals and shall evaluate that information against the instructions provided by the classification guidance or the markings on source documents.

b. Drafters of derivatively classified documents shall portion-mark their drafts and keep records of the sources they use, to facilitate derivative classification of the finished product.

c. When material is derivatively classified based on “multiple sources” (i.e., more than one security classification guide, classified source document, or combination thereof), the derivative classifier shall compile a list of the sources used. This list shall be included in or attached to the document.

d. Duration of classification for derivatively classified documents shall be determined in accordance with section 13 of this enclosure and applied in accordance with Volume 2 of this Manual. The instructions shall not be automatically copied from source documents without consideration of adjustments that may be required (e.g., due to use of multiple sources, changes in policy, changes in classification guidance).

e. If extracting information from a document or section of a document classified by compilation, the derivative classifier shall consult the explanation on the source document to determine the appropriate classification. If that does not provide sufficient guidance, the derivative classifier shall contact the originator of the source document for assistance.

f. Infrequently, different sources of classification guidance may specify different classification for the same information. When such inconsistencies are encountered, the derivative classifier must contact the applicable OCA(s) for resolution of the inconsistency. Pending determination, the document or material containing the information shall be protected at the highest level of classification specified by the sources.

13. DURATION OF CLASSIFICATION. Every time a classified document is created, a determination must be made regarding how long the information is to be protected (i.e., when the information will lose its sensitivity and no longer merit or qualify for classification). This is an essential part of the classification process.

...

2314 a. Originally Classified Information. At the time an item of information is classified, the
 2315 OCA shall establish a specific date or event for declassification, based on the duration of the
 2316 national security sensitivity of the information. The OCA shall use one of the following duration
 2317 options, selecting, whenever possible, the one that will result in the shortest duration of
 2318 classification.

2319
 2320 (1) A date or independently verifiable event less than 10 years from the date of original
 2321 classification*;

2322
 2323 (2) A date 10 years from the date of original classification*;

2324
 2325 (3) A date or independently verifiable event greater than 10 and less than 25 years from the
 2326 date of original classification*;

2327
 2328 (4) A date 25 years from the date of original classification*;

2329
 2330 (5) "50X1-HUM," designating a duration of up to 75 years from the date of original
 2331 classification, when classifying information that could clearly and demonstrably be expected to
 2332 reveal the identity of a confidential human source or a human intelligence source;

2333
 2334 (6) "50X2-WMD," designating a duration of up to 75 years from the date of original
 2335 classification, when classifying information that could clearly and demonstrably be expected to
 2336 reveal key design concepts of weapons of mass destruction; or

2337
 2338 (7) "25X" with date or event, designating a duration of up to 50 years from the date of
 2339 original classification, when classifying information that clearly falls within an exemption from
 2340 automatic declassification at 25 years that has previously been approved by the ISCAP.

2341
 2342 b. Derivatively Classified Information. For derivatively classified information, the most
 2343 restrictive declassification instruction (i.e., the one that specifies the longest duration of
 2344 classification) must be carried forward from the source document(s), security classification guide(s)
 2345 or other classification guidance provided by the OCA. Specific guidance on determining the most
 2346 restrictive instruction is provided in Enclosure 3 of Volume 2.

2347
 2348 c. Extending the Duration of Classification. Information is declassified on the date or event
 2349 specified by the OCA unless the OCA takes action to extend the duration of classification.

2350
 2351 (1) If the date or event for declassification specified by the OCA has not passed, an OCA
 2352 may extend the duration of classification for information under their jurisdiction, provided the
 2353 information continues to meet the standards for classification. The period of classification shall not
 2354 exceed 25 years from the date of the document's origin. When extending the duration of
 2355 classification, the OCA must immediately notify all known holders of the information of the
 2356 extension.

2357
 2358 (2) If the date or event specified by the OCA has passed, the information may be
 2359 reclassified only in accordance with sections 17 and 18 of this enclosure.

2360
 2361
 2362 14. FORMAT FOR DISSEMINATION. Whenever practicable, OCAs and derivative classifiers

...

2363 shall use a classified attachment, addendum, annex, enclosure, or similar section if the classified
2364 information constitutes only a small portion of an otherwise unclassified document. Alternately, a
2365 separate product that would allow dissemination at the lowest level of classification possible or in
2366 unclassified form may be prepared.

2367
2368

2369 15. COMPILATIONS

2370

2371 a. Compilations of information that are individually unclassified (or classified at a lower
2372 level) may be classified (or classified at a higher level) only if the compiled information reveals an
2373 additional association or relationship that:

2374

2375 (1) Qualifies for classification pursuant to paragraph 1.b. of this enclosure; and

2376

2377 (2) Is not otherwise revealed by the individual elements of information.

2378

2379 b. OCAs shall use the same decision process as for other information when determining
2380 whether compilations of individual items require classification.

2381

2382 (1) Classification as a result of compilation must meet the same criteria in terms of
2383 justification as other original classification actions (see section 6 of this enclosure).

2384

2385 (2) The information must be located where one could realistically assume that the
2386 elements of information could be associated to derive classified meaning. Note that user queries of
2387 data in electronic formats (e.g., databases, spreadsheets) lead to new aggregations, and posting of
2388 information on the Internet makes the use of data mining and other data correlation tools easy and
2389 widespread. OCAs should consider the possibility that such tools and methods will be used to
2390 compile information and should, when appropriate, identify classified compilations when issuing
2391 classification guidance.

2392

2393 c. Classification as a result of compilation requires an original classification decision by an
2394 authorized OCA or classification guidance issued by an OCA (e.g., a security classification guide).

2395

2396 (1) The final decision regarding classification of compiled data resides with the OCA who
2397 has purview over the program that creates or generates the compilation. However, the program
2398 manager or other official responsible for the database, application, or program that creates or
2399 generates the compilation is responsible for facilitating, as necessary, a security classification
2400 review with other appropriate OCAs for the constituent items of information. Assistance from the
2401 servicing security, OPSEC, and CI offices is recommended, but the responsibility for the review
2402 resides with the program manager or other responsible official. Where the individual OCAs are
2403 unable to agree on the classification of the aggregated data, the decision may be raised to an official
2404 higher in the chain of command who is authorized OCA and has program or supervisory authority
2405 over the data.

2406

2407 (2) A classification by compilation decision must honor (i.e., cannot overrule or change)
2408 previous decisions by an OCA regarding the classification of individual elements or of the
2409 compilation. As part of the classification decision process, officials should determine whether the
2410 compilation has previously been classified by another OCA.

2411

...

2412 (3) OCAs must avoid using classification as a means to protect information merely
 2413 because the compiled data represents a significant amount of information available in one place
 2414 (e.g., in an authoritative data source), unless damage to the national security can be articulated as
 2415 required by section 6 of this enclosure. When information qualifies for classification as a result of
 2416 compilation, it is because the whole is greater than the sum of the parts (i.e., something new is
 2417 revealed by putting all of the pieces together that is not revealed by the individual parts).
 2418 Classification of compilations presents its own set of issues, not the least of which is determining
 2419 how to handle and share individual pieces of information without creating the possibility for
 2420 inadvertent compilation of the whole.

2421
 2422 (4) The classification of each element of a classified compilation must be clearly
 2423 identified by portion marking or explanation, as appropriate, so that when separated the
 2424 classification of each individual element can be determined. OCAs are reminded of the
 2425 requirement to clearly describe the basis for the classification as a result of compilation when
 2426 originally classifying the compilation (see marking requirements in section 12, Enclosure 3 of
 2427 Volume 2 of this Manual). If the classification of an individual element cannot be determined, the
 2428 information shall be protected at the level of classification of the compilation and the OCA
 2429 contacted for specific guidance.

2430
 2431 d. When specific combinations of unclassified data elements are known to be classified (or
 2432 specific combinations of data elements classified at a lower level qualify for classification at a
 2433 higher level), the OCA must identify these combinations and document them in security
 2434 classification guides. The program manager or other responsible official and the OCA(s) should
 2435 review the elements of information used by their program(s) as early in the program as possible to
 2436 determine if there are obvious or likely compilations that reveal relationships or associations that
 2437 require classification.

2438
 2439 e. Where specific combinations of unclassified data elements are known to be classified,
 2440 CONSISTENTLY withholding specified data elements from public Internet posting and, to the
 2441 extent possible consistent with statute and other regulations, public release can mitigate the ability
 2442 of others to create the classified compilation. Thus, OCAs should consider including in security
 2443 classification guides, where appropriate, prohibitions on posting one or more of the specific data
 2444 elements that are known to make up a classified compilation of unclassified data elements to
 2445 publicly accessible Internet sites.

2446
 2447
 2448 16. CLASSIFICATION OF ACQUISITION INFORMATION. Classifying information involved
 2449 in the DoD acquisition process shall conform to the requirements of DoDD 5000.01 (Reference
 2450 (az)) and DoDI 5000.02 (Reference (ba)), as well as this enclosure. Security classification guides
 2451 should be updated to include classified critical program information identified as part of the
 2452 program protection planning process required by DoDI 5200.39 (Reference (bb)).

2453
 2454
 2455 17. CLASSIFICATION OF INFORMATION RELEASED TO THE PUBLIC

2456
 2457 a. Classified Information Released Without Proper Authority

2458
 2459 (1) Classified information that has been released to the public without proper authority
 2460 (e.g., media leak, data spill) remains classified. It may be declassified upon determination by the

...

2461 appropriate OCA. Enclosure 6 of Volume 3 of this Manual identifies issues to be considered when
2462 making the decision. When the determination is made that the information will remain classified,
2463 the appropriate OCA will notify known authorized holders accordingly and provide the following
2464 marking guidance to be used in the event the information is not marked:

2465

2466 (a) Overall level of classification;

2467

2468 (b) Portion markings;

2469

2470 (c) Identity, by name or personal identifier and position, of the OCA;

2471

2472 (d) Declassification instructions;

2473

2474 (e) Concise reason for classification; and

2475

2476 (f) Date the action was taken.

2477

2478 (2) Holders of the information shall take administrative action, as needed, to apply
2479 markings and controls. DoD personnel shall not publicly acknowledge the release of classified
2480 information and must be careful not to make any statement or comment that confirms the accuracy
2481 of or verifies the information requiring protection.

2482

2483 (3) ***(Added)(DAF) If the information released to the public contains RD, FRD,**
2484 **CNWDI, DOE Sigma, or TFNI, notify AF/A10, as soon as possible. (T-1).**

2485

2486 b. Reclassification of Information Declassified and Released to the Public Under Proper
2487 Authority

2488

2489 (1) Information that has been declassified and released to the public under proper
2490 authority may be reclassified only when:

2491

2492 (a) The information may be reasonably recoverable without bringing undue attention
2493 to the information, which means that:

2494

2495 1. Most individual recipients or holders are known and can be contacted and all
2496 forms of the information to be reclassified can be retrieved from them.

2497

2498 2. If the information has been made available to the public via means such as
2499 U.S. Government archives or reading rooms, it can be or has been withdrawn from public access
2500 without significant media or public attention or notice.

2501

2502 (b) The Secretary of Defense approves the reclassification based on a document-by-
2503 document determination and recommendation by the Head of the originating DoD Component,
2504 other than the Secretary of a Military Department, when that reclassification of the information is
2505 required to prevent significant and demonstrable damage to the national security. Reclassification
2506 and release of information under proper authority means the DoD Component with jurisdiction over
2507 the information authorized declassification and release of the information. The Secretaries of a
2508 Military Department shall approve the reclassification of information under their jurisdiction on the
2509 same basis and shall notify the USD(I&S) of the action. The Military Departments shall provide

2510 implementing guidance to their subordinate activities for submitting such requests.

2511
2512 (2) DoD Component Heads other than the Secretaries of the Military Departments shall
2513 submit recommendations for reclassification of information under their jurisdiction to the Secretary
2514 of Defense through the USD(I&S). Recommendations for reclassification must include, on a
2515 document-by-document basis:

2516
2517 (a) A description of the information.

2518
2519 (b) All information necessary for the original classification decision in accordance
2520 with section 6 of this enclosure, including classification level of the information and
2521 declassification instructions to be applied.

2522
2523 (c) When and how it was released to the public.

2524
2525 (d) An explanation as to why it should be reclassified. Include the applicable reason in
2526 accordance with Reference (d) and describe what damage could occur to national security. Also
2527 describe what damage may have already occurred as a result of the release.

2528
2529 (e) The number of recipients and/or holders and how they will be notified of the
2530 reclassification.

2531
2532 (f) How the information will be recovered.

2533
2534 (g) Whether the information is in the custody of NARA and whether the Archivist of
2535 the United States must be notified of the reclassification as specified in subparagraph 17.b.(4) of this
2536 section.

2537
2538 (3) Once a reclassification action has occurred, it must be reported to all recipients and
2539 holders, to the Assistant to the President for National Security Affairs (herein after referred to as
2540 “the National Security Advisor”) and to ISOO within 30 days. The notification to ISOO must
2541 include how the “reasonably recoverable” decision was made, including the number of recipients or
2542 holders, how the information was recovered, and how the recipients and holders were notified.

2543
2544 (a) The Secretaries of the Military Departments shall notify the National Security
2545 Advisor and ISOO directly and provide an information copy to the USD(I&S). The Secretary of
2546 Defense, after making reclassification decisions, will notify the National Security Advisor and
2547 ISOO of such decisions.

2548
2549 (4) For documents in the physical and legal custody of NARA that have been available for
2550 public use, reclassification must also be reported to the Archivist of the United States, who shall
2551 suspend public access pending approval of the reclassification action by the Director, ISOO. The
2552 Secretaries of the Military Departments shall notify the Archivist directly and provide an
2553 information copy to USD(I&S). The Secretary of Defense will notify the Archivist as required for
2554 decisions involving other DoD Components. Disapproval of the reclassification action by the
2555 Director, ISOO, may be appealed to the President through the National Security Advisor. Public
2556 access shall remain suspended pending decision on the appeal.

2557
2558 (a) OCAs shall notify the Secretary of Defense of the need to appeal ISOO decisions

2559 through their DoD Component Head and the USD(I&S).

2560
2561 (b) Notifications shall clearly articulate the compelling national security reasons for
2562 reclassifying the information and shall counter the ISOO rationale for disapproving the
2563 reclassification.

2564
2565 (5) Once a final decision is rendered, OCAs shall update their security classification
2566 guidance accordingly. The reclassified information must be marked and safeguarded in accordance
2567 with the requirements of Volumes 2 and 3 of this Manual.

2568
2569 (6) Any cleared recipients or holders of reclassified information shall be notified and
2570 appropriately briefed about their continuing legal obligations and responsibilities to protect this
2571 information from unauthorized disclosure. The recipients or holder who do not have security
2572 clearances shall, to the extent practicable, be appropriately briefed about the reclassification of the
2573 information to which they have had access and their obligation not to disclose the information, and
2574 shall be asked to sign an acknowledgement of the briefing and to return all copies of the
2575 information in their possession.

2576
2577 c. Information Declassified and Released to the Public without Proper Authority. Information
2578 that was declassified without proper authority remains classified. See paragraph
2579 17.a. of this enclosure and paragraph 1.c. of Enclosure 5 of this Volume.

2580
2581
2582 18. CLASSIFICATION OR RECLASSIFICATION FOLLOWING RECEIPT OF A REQUEST
2583 FOR INFORMATION. Information that has not previously been released to the public under
2584 proper authority may be classified or reclassified after receiving a request for it under FOIA;
2585 section 2204(c)(1) of Reference (av) (also known as “The Presidential Records Act of 1978”);
2586 section 552a of Reference (ay) (also known and hereinafter referred to as “The Privacy Act of
2587 1974, as amended”); or the mandatory review provisions of section 3.5 of Reference (d), only if it
2588 is done on a document-by-document basis with the personal participation or under the direction of
2589 the USD(I&S), the Secretary or Under Secretary of a Military Department, or the senior agency
2590 official appointed within a Military Department in accordance with section 5.4(d) of Reference (d).
2591 OCAs shall submit requests to the USD(I&S) through the Head of the DoD Component.

2592
2593 a. The provisions of this section apply to information that has been declassified in accordance
2594 with the date or event specified by the OCA as well as to information not previously classified.

2595
2596 b. Classification requests shall provide all information necessary for the original classification
2597 process as specified by section 6 of this enclosure.

2598
2599 c. The Secretaries of the Military Departments shall notify the USD(I&S) of classification
2600 decisions made in accordance with the provisions of this section.

2601
2602 d. Once a decision is rendered, OCAs shall update their security classification guidance as
2603 needed.

2604
2605
2606 19. CLASSIFYING NON-GOVERNMENT RESEARCH AND DEVELOPMENT
2607 INFORMATION

...

2608

2609 a. Information that is a product of contractor or individual independent research and
2610 development (IR&D) or bid and proposal (B&P) efforts, as defined by DoDI 3204.01 (Reference
2611 (bc)), conducted without prior or current access to classified information associated with the
2612 specific information in question, may not be classified unless:

2613

2614 (1) The U.S. Government first acquires a proprietary interest in the information; or,

2615

2616 (2) The contractor or individual conducting the IR&D or B&P requests that the U.S.
2617 Government contracting activity place the information under the control of the security
2618 classification system without relinquishing ownership of the information.

2619

2620 b. The contractor or individual conducting such an IR&D or B&P effort and believing that the
2621 information generated may require protection in the interest of national security shall safeguard the
2622 information and submit it to an appropriate U.S. Government activity for a classification
2623 determination.

2624

2625 (1) The U.S. Government activity receiving the request shall issue security classification
2626 guidance, as appropriate, if the information is to be classified. If the information is not under the
2627 activity's classification authority, the activity shall refer the matter to the appropriate classification
2628 authority and inform the individual or contractor of the referral. The information shall be
2629 safeguarded until the matter is resolved.

2630

2631 (2) The U.S. Government activity authorizing classification for the information shall
2632 verify whether the contractor or individual is cleared and has been authorized to store classified
2633 information. If not, the U.S. Government activity authorizing classification shall advise whether
2634 security clearance action should be initiated.

2635

2636 (3) If the contractor or individual refuses to be processed for the appropriate security
2637 clearance and the U.S. Government does not acquire a proprietary interest in the information, the
2638 information may not be classified.

2639

2640 (4) If the information is not classified, consideration may be given to the need for other
2641 controls applicable to unclassified information (e.g., export controls) (See DoDI 5200.48 for
2642 guidance on CUI).

2643

2644

2645 20. THE PATENT SECRECY ACT OF 1952. Sections 181 through 188 of title 35, U.S.C. (also
2646 known and hereinafter referred to as "The Patent Secrecy Act of 1952" (Reference (bd)) provides
2647 that the Secretary of Defense, among others, may determine that disclosure of an invention by
2648 granting of a patent would be detrimental to the national security. The Department of Defense shall
2649 handle a patent application on which a secrecy order has been imposed as follows:

2650

2651 a. If the patent application contains information that warrants classification, it shall be
2652 assigned a classification and be marked and safeguarded commensurate with the level of
2653 classification.

2654

2655 b. Unclassified patent applications that do not contain information that warrants classification,
2656 but requires CUI safeguarding and dissemination controls, will be marked as a category of CUI in

...

2657 accordance with DoDI 5200.48. This same requirement applies to legacy patent applications
2658 marked with the former statement that required handling as CONFIDENTIAL.

2659
2660
2661 21. REQUESTS FOR CLASSIFICATION DETERMINATION. Within 30 days of receipt
2662 OCAs shall provide a classification determination to requests for same from individuals who are
2663 not OCAs, but who believe they have originated information requiring classification. If the
2664 information is not under the OCA's classification authority, the request shall be referred to the
2665 appropriate OCA and the requestor shall be informed of the referral. Pending a classification
2666 determination the information shall be protected consistent with the requirements of this Manual.

2667

2668

2669 22. CHALLENGES TO CLASSIFICATION

2670

2671 a. Principles. If holders of information have substantial reason to believe that the information
2672 is improperly or unnecessarily classified, they shall communicate that belief to their security
2673 manager or the OCA to bring about any necessary correction. This may be done informally or by
2674 submitting a formal challenge to the classification in accordance with References (d) and (f).

2675

2676 (1) Informal questioning of classification is encouraged before resorting to formal
2677 challenge. If the information holder has reason to believe the classification applied to information is
2678 inappropriate, he or she should contact the classifier of the source document or material to resolve
2679 the issue.

2680

2681 (2) The Heads of the DoD Components shall ensure that no retribution is taken against
2682 any individual for questioning a classification or making a formal challenge to a classification.

2683

2684 (3) Formal challenges to classification made pursuant to this section shall include
2685 sufficient description of the information being challenged to permit identification of the
2686 information and its classifier with reasonable effort. Challenges to classification made by DoD
2687 personnel shall also include the reason why the challenger believes that the information is
2688 improperly or unnecessarily classified. The challenge shall be unclassified, if possible.

2689

2690 (4) Pending final decision on the classification level, the information that is the subject of
2691 a classification challenge will remain classified at its current classification level or the
2692 recommended change level, whichever is higher. The information will continue to be safeguarded
2693 unless and until a decision is made to declassify it.

2694

2695 (5) The provisions of this section do not apply to information required to be submitted for
2696 prepublication review or other administrative process pursuant to an approved NDA.

2697

2698 (6) **(Added)(DAF) Formal classification challenges must be routed through the**
2699 **MAJCOM/FLDCOM IP for staffing. (T-1). Refer all classification challenges of RD or FRD**
2700 **to AF/A10.**

2701

2702 b. Procedures. The Heads of the DoD Components shall encourage classification challenges
2703 and establish procedures for handling challenges to classification received from within and from
2704 outside their Components in accordance with Reference (f). The DoD Components shall:

2705

2706 (1) Incorporate the following language for Component security classification guides
2707 consistent with the intent of Section 5.3 of Reference (d):

2708
2709 (a) Follow the guidance provided in Paragraph 22 of this enclosure for individuals
2710 who wish to challenge information they believe has been improperly or unnecessarily classified.

2711
2712 (b) Such challenges are encouraged, and expected, and should be forwarded through
2713 the appropriate channels to the office of primary responsibility.

2714
2715 (c) Pending final decision, handle and protect the information at its current
2716 classification level or at the recommended change level, whichever is higher.

2717
2718 (d) Challenges should include sufficient description to permit identification of the
2719 specific information under challenge with reasonable effort.

2720
2721 (e) Challenges should include detailed justification outlining why the information is
2722 improperly or unnecessarily classified.

2723
2724 (2) Establish a system for processing, tracking, and recording formal challenges to
2725 classification, including administrative appeals of classification decisions, and ensure that DoD
2726 Component personnel are made aware of the established procedures for classification challenges.

2727
2728 (3) Provide an opportunity for review of the information by an impartial official or panel.

2729
2730 (4) Except as provided in subparagraphs 22.b. (5) and (6) of this section, provide an initial
2731 written response to each challenge within 60 days. If not responding fully to the challenge within
2732 60 days, the DoD Component shall acknowledge the challenge and provide an expected date of
2733 response. This acknowledgment shall include a statement that, if no response is received within
2734 120 days, the challenger has the right to forward the challenge to the ISCAP for decision. The
2735 challenger may also forward the challenge to the ISCAP if the Component has not responded to an
2736 appeal within 90 days of receipt of the appeal. DoD Component responses to those challenges it
2737 denies shall include the challenger's right to appeal to the ISCAP.

2738
2739 (5) Not process the challenge if it concerns information that has been the subject of a
2740 challenge within the preceding two (2) years or is the subject of pending litigation. The DoD
2741 Component shall inform the challenger of the situation and appropriate appellate procedures.

2742
2743 (6) Refer challenges involving RD to the Department of the Energy and FRD to the Deputy
2744 Assistant Secretary of Defense, Nuclear Matters (DASD(NM)) and notify the challenger
2745 accordingly. Do not include a statement about forwarding the challenge to the ISCAP in the
2746 notification letter, as these categories of information are not within the purview of the ISCAP.

2747
2748 (7) In case a classification challenge involves documents that contain RD and/or FRD as
2749 well as information classified under Reference (d), delete (redact) the RD and FRD portions of the
2750 documents before the document is forwarded to the ISCAP for review.

ENCLOSURE 5DECLASSIFICATION AND CHANGES IN CLASSIFICATION1. DECLASSIFICATION POLICY

a. Per Reference (d), information shall be declassified as soon as it no longer meets the standards for classification. In some exceptional cases, the need to protect information still meeting these standards may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. Pursuant to DoD policy in Reference (b), information shall remain classified only as long as:

- (1) It is in the best interest of national security to keep it protected.
- (2) Continued classification is in accordance with the requirements of Reference (d).

b. If DoD officials have reason to believe that the public interest in disclosure of information outweighs the need for continued classification, they shall refer the matter to the appropriate senior agency official appointed in accordance with section 5.4(d) of Reference (d), who shall consult with the OCA. The senior agency official shall determine whether to declassify the information.

c. Classified information that has been declassified without proper authority remains classified until declassified by an OCA with jurisdiction over the information.

- (1) Administrative action shall be taken to restore markings and controls, as appropriate.
- (2) If the information is in records in the physical and legal custody of NARA and has been made available to the public:

(a) The OCA shall, as part of determining if restoration of markings and controls is appropriate, consider whether removing the information from public access will significantly mitigate harm to the national security or otherwise draw undue attention to the information.

(b) DoD or Military Department senior agency official shall provide written notification to the Archivist of the U.S., which shall include a description of the record(s), the elements of information that are classified, the duration of classification, and the specific authority for continued classification. OCAs in DoD Components other than the Military Departments shall submit notifications to USD(I&S), through their chain of command, for submission to the Archivist.

(c) The issue shall be referred to the Director, ISOO if the information is more than 25 years old and the Archivist does not agree with the OCA's determination that the information remains classified. The information shall be withdrawn from public access pending resolution.

d. Classified information shall be marked as declassified, as specified by Enclosure 3 of Volume 2 of this Manual, before it is handled as unclassified. Holders of classified information

2800 marked with a date or event on the “declassify on” line shall, when the date or event has passed,
 2801 confirm that the OCA(s) of the information has not extended the classification period. This can
 2802 be done by reference to a security classification or declassification guide or to other appropriate
 2803 guidance issued by the OCA or by consultation with the OCA. Once declassification is
 2804 confirmed, such information may be made publicly available only as provided in paragraph 1.e
 2805 of this section.

2806
 2807 e. Declassification does not authorize release of the information to the public.
 2808 DECLASSIFIED INFORMATION SHALL NOT BE RELEASED TO THE PUBLIC UNTIL A
 2809 PUBLIC RELEASE REVIEW, AS REQUIRED BY REFERENCES (v) AND (w,) HAS BEEN
 2810 CONDUCTED to determine if there are reasons for withholding some or all of the information.
 2811 Declassified information may be released to the public unless withholding is appropriate in
 2812 accordance with other applicable law (for example, FOIA or the Privacy Act of 1974, as
 2813 amended) or DoD issuance (for example, Reference (v) and DoDD 5230.25 (Reference (be))).
 2814 Regardless of the date specified for declassification, declassified information shall not be
 2815 approved for public release without referral to the OCA of the information, except records
 2816 accessioned by NARA that were reviewed for automatic declassification in accordance with
 2817 section 3.3 of Reference (d) will be reviewed by NARA for public release.

2818
 2819 f. Personnel leaving DoD employment or service may not direct that information be
 2820 declassified in order to remove it from DoD control.

2821
 2822 g. OCAs affected by ISCAP deliberations shall be notified of the final decision and shall
 2823 consider the need to change classification and declassification guides to reflect the specific
 2824 ISCAP decision.

2825
 2826
 2827 2. PROCESSES FOR DECLASSIFICATION. Reference (d) establishes four separate and
 2828 parallel processes for declassifying information:

2829
 2830 a. A process requiring the original classifier to decide at the time information is classified
 2831 when it may be declassified.

2832
 2833 b. A process that shall cause information of permanent historical value to be automatically
 2834 declassified no later than 31 December of the year that is 25 years from the date of its origin
 2835 unless specific action is taken to keep it classified.

2836
 2837 c. A process for reviewing information for possible declassification upon request (mandatory
 2838 declassification review).

2839
 2840 d. A process for systematic review of information for possible declassification.

2841
 2842
 2843 3. AUTHORITY TO DECLASSIFY

2844
 2845 a. Information may be declassified or downgraded by the cognizant OCA, by supervisory
 2846 officials of the OCA if the supervisory official has OCA, or by those officials who have been
 2847 delegated declassification authority in accordance with paragraph 3.b. of this enclosure. The
 2848 authority to declassify information extends only to information for which the specific official has

2849 classification, program, or functional responsibility.

2850
2851 b. DoD Component Heads with OCA may designate officials within their organizations to
2852 exercise declassification authority (e.g., make declassification decisions, issue declassification
2853 guidance) over specific types or categories of information for which they are responsible.
2854 Delegations of declassification authority shall be reported concurrently to the Director of
2855 Security, USD(I&S). Other OCAs may designate members of their staffs to exercise
2856 declassification authority over information under their jurisdiction. Declassification
2857 authorities, other than original classifiers, shall receive training as specified in section 6 of
2858 Enclosure 5, Volume 3 of this Manual upon initial designation and every two (2) years
2859 thereafter.

2860
2861 c. Pursuant to section 7 of this enclosure, only NSA/CSS is authorized to downgrade or
2862 declassify cryptologic information.

2863
2864 d. If the activity originating the classified information no longer exists, the activity that
2865 inherited the functions of the originating activity shall determine what constitutes appropriate
2866 declassification action. If the functions of the originating activity were dispersed to more than
2867 one activity, the inheriting activity(ies) cannot be determined, or the functions have ceased to
2868 exist, the senior agency official of the DoD Component of the originating activity shall
2869 determine the declassification action to be taken.

2870
2871 e. Information originated by another agency or DoD Component shall be referred to the
2872 originator for downgrading or declassification determinations.

2873
2874 f. Declassification of information is an inherently governmental function that must be
2875 performed by a properly trained and authorized U.S. Government employee having the explicit
2876 permission of the government organization that originated the information. DoD Components
2877 must organize for and provide adequate resources to execute this mission while protecting the
2878 national security. Contractors may perform routine administrative, pre-processing, and
2879 technology support functions, as well as make recommendations for declassification of
2880 information. U.S. Government personnel must sample contractors' declassification
2881 recommendations at a rate of no less than five (5) percent of the total volume of records being
2882 processed for declassification, before making the formal decision to declassify the information.

2883
2884 **g. (Added)(DAF) The Air Force Declassification Office (AFDO) provides oversight for**
2885 **all DAF automatic, systematic and National Archives reviews for declassification matters.**
2886 **AFDO will:**

2887
2888 **(1) (Added)(DAF) Ensure DAF personnel conducting automatic, systematic and/or**
2889 **National Archives reviews for declassification receive training, as specified in volume 3,**
2890 **enclosure 5, of this Manual, and every two (2) years thereafter. Develop and conduct training**
2891 **in declassification, equity recognition and nuclear weapons information protection, as**
2892 **required.**

2893
2894 **(2) (Added)(DAF) Review DAF originated records greater than 25 years old, subject**
2895 **to automatic declassification, and located at the National Archives at College Park, MD**
2896 **(Archives II). This also includes other agency records at Archives II, which contain DAF**
2897 **equities.**

2898
2899 **(3) (Added)(DAF) Review DAF-owned records stored at the Washington National**
2900 **Records Center, in Suitland, MD.**

2901
2902 **(4) (Added)(DAF) Provide trained reviewers to the National Declassification Center,**
2903 **at Archives II location.**

2904
2905 **(5) (Added)(DAF) Prepare and maintain the DAF declassification guide for historical**
2906 **records. Assist with historical document, publication and manuscript classification reviews,**
2907 **as requested.**

2908
2909 **(6) (Added)(DAF) Conduct environmental archival research for the DAF**
2910 **Environmental Law and Litigation Division, to support environmental litigation, as**
2911 **requested.**

2912
2913 **(7) *(Added)(DAF) DAF OCAs, MDR officials and declassification officers**
2914 **cannot declassify RD, FRD, CNWDI, DOE Sigma, or TFNI.**

2915
2916
2917 4. DECLASSIFICATION GUIDANCE. Persons with declassification authority shall develop
2918 and issue declassification guidance to facilitate effective review and declassification of information
2919 classified under both current and previous classified national security information Executive orders.
2920 The guidance may be in the form of declassification guides, sections of security classification
2921 guides, memorandums, etc. Exemptions authorized in accordance with section 13 of this enclosure
2922 should be cited in declassification guidance.

2923
2924
2925 5. DECLASSIFICATION OF INFORMATION

2926
2927 a. Holders of classified information marked with a date or event on the “declassify on” line,
2928 shall, prior to downgrading or declassifying the information, confirm that the OCA(s) for the
2929 information has not extended the classification period.

2930
2931 b. Holders of classified information may confirm the classification period (i.e., date or event
2932 for declassification) by reference to the applicable security classification or declassification guide
2933 or other appropriate guidance issued by the OCA(s), or by consultation with the OCA(s). Classified
2934 information shall continue to be safeguarded as required for the indicated classification level until
2935 the holder has confirmed that the OCA(s) has not extended the classification period.

2936
2937 c. If the holder of a document has reason to believe it should not be declassified as specified,
2938 the originator shall be notified through appropriate administrative channels. The document or
2939 material shall continue to be protected at the originally assigned classification until the issue is
2940 resolved.

2941
2942 d. Declassification markings are used to clearly convey the declassified status of the
2943 information and who authorized the declassification. All declassified information in agency
2944 records not held by NARA shall have the declassification markings required by Enclosure 3 of
2945 Volume 2 of this Manual applied.

...

2947
2948 6. CANCELING OR CHANGING CLASSIFICATION MARKINGS. Declassification authority
2949 is not required for simply canceling or changing classification markings in accordance with
2950 guidance from an OCA or declassification authority. Sections 18 and 19 of this enclosure provide
2951 guidance on downgrading and upgrading classified information.

2952
2953
2954 7. SPECIAL PROCEDURES FOR CRYPTOLOGIC INFORMATION. Only NSA/CSS may
2955 declassify cryptologic information. Therefore, such information uncovered in systematic or
2956 mandatory review of U.S. Government records for declassification, including such information
2957 incorporated into other documents, must be referred to the NSA/CSS for declassification
2958 determination.

2959
2960 a. Recognition of cryptologic information is not always easy since it may concern or reveal
2961 the processes, techniques, operations, and scope of signals intelligence, which consists of
2962 communications intelligence, electronic intelligence, and foreign instrumentation signals
2963 intelligence, or it may concern IA, which includes COMSEC, including the communications
2964 portion of cover and deception plans. Much cryptologic information is also considered FGI.

2965
2966 b. NSA/CSS has established special procedures for mandatory review for declassification of
2967 classified cryptologic information. For questions regarding cryptographic equities or for referrals
2968 for declassification determination, contact:

2969
2970 Director, National Security
2971 Agency/ Chief, Central Security Service
2972 ATTN: Declassification Services
2973 (DJP5) Fort George G. Meade, MD 20755-6248

2974
2975

2976 8. PERMANENTLY VALUABLE RECORDS

2977
2978 a. Classified information in records that are scheduled for retention by NARA as permanently
2979 valuable records when that information is less than 20 years old shall be subject to the automatic
2980 declassification provisions of section 12 of this enclosure when the information is 25 years old.

2981
2982 b. Classified information in records that are scheduled for retention by NARA as permanently
2983 valuable records when that information is already more than 20 years old shall be subject to the
2984 automatic declassification provisions of section 12 of this enclosure 5 years from the date the
2985 records are scheduled.

2986
2987

2988 9. RECORDS DETERMINED NOT TO HAVE PERMANENT HISTORICAL VALUE.

2989 Classified records determined not to be permanently valuable and not scheduled retention by
2990 NARA are subject to the automatic declassification provisions of this issuance. The disposition
2991 (destruction) date of those records in the DoD Component's Records Control Schedule or General
2992 Records Schedule approved by NARA shall be used as the declassification date, although the
2993 duration of classification may be extended if a record has been retained for business reasons beyond
2994 its scheduled destruction date. If the disposition date extends beyond 25 years, an exemption
2995 request must be submitted to and approved by the ISCAP in accordance with the procedure in

2996 section 13 of this enclosure.

2997

2998

2999

10. EXTENDING CLASSIFICATION BEYOND 25 YEARS FOR UNSCHEDULED

3000

RECORDS. For unscheduled classified records (both permanent and temporary), the duration of

3001

classification beyond 25 years shall be determined when the records are scheduled (i.e., when

3002

NARA has approved a records control schedule that can be used to determine their final

3003

disposition). Permanently valuable records must be scheduled before they are 25 years old in order

3004

to request ISCAP approval to extend classification beyond 25 years when applicable. Contact the

3005

DoD Component Records Manager for further guidance on scheduling records.

3006

3007

3008

11. CLASSIFIED INFORMATION IN THE CUSTODY OF CONTRACTORS, LICENSEES,

3009

GRANTEES, OR OTHER AUTHORIZED PRIVATE ORGANIZATIONS OR INDIVIDUALS.

3010

Pursuant to the provisions of Reference (ab), DoD Components must provide security classification

3011

and declassification guidance to contractors, licensees, grantees, or other authorized private

3012

organizations or individuals who possess DoD classified information. DoD Components must also

3013

determine if classified records are held by such entities, and, if so, whether they are permanent

3014

records of historical value and thus subject to automatic declassification. Until such a

3015

determination has been made by an appropriate official, the classified information contained in

3016

such records shall not be subject to automatic declassification and shall be safeguarded in

3017

accordance with the most recent security classification or declassification guidance provided by the

3018

DoD Component.

3019

3020

3021

12. AUTOMATIC DECLASSIFICATION. Reference (d) establishes a system for

3022

declassification of information in permanently valuable historical records. DoD Component

3023

declassification activities shall conduct reviews of records eligible for automatic declassification in

3024

accordance with the procedures specified in this enclosure and Reference (f) and by the NDC.

3025

3026

a. Deadline. All permanently valuable records shall be reviewed for declassification by

3027

December 31 of the year in which they become 25 years old. Unless the document warrants

3028

continued classification in accordance with an authorized exclusion (see paragraph 12.e of this

3029

section) or an ISCAP-approved exemption (see section 13 of this enclosure), or qualifies for a delay

3030

of automatic declassification in accordance with paragraph 12.g. of this section, the documents

3031

shall be declassified.

3032

3033

(1) Documents not reviewed by December 31 of the year in which they become 25 years

3034

old shall be automatically declassified unless the onset of automatic declassification has been

3035

delayed in accordance with paragraph 12.g. of this section or an exemption has been approved.

3036

3037

(2) Documents exempted from declassification shall be automatically declassified on

3038

December 31 of the year in which they become 50 years old or, as appropriate, 75 years old unless

3039

further exempted from declassification in accordance with section 13 of this enclosure.

3040

3041

(3) If the document's date of origin cannot be readily determined, the date of original

3042

classification shall be used to determine the automatic declassification deadline.

3043

3044

b. Secretary of Defense Certification. In addition to the requirement of paragraph 12.a. of this

...

3045 section, DoD Components shall not automatically declassify DoD records without reviewing them
3046 for declassification unless the Secretary of Defense has certified to Congress that such
3047 declassification would not harm the national security pursuant to section 1041(c) of Public Law
3048 106-65 (Reference (bf)). If records will not be reviewed for declassification as required prior to
3049 December 31 of the year in which they become 25 years old, the DoD Component Heads shall
3050 notify the USD(I&S), 6 months in advance of the deadline, so the required Secretary of Defense
3051 certification can be addressed. Notification shall include identification of the records, the
3052 compelling reason why the records will not be reviewed by the deadline, how many records will
3053 remain un-reviewed, where the records are located, and when the required reviews will be
3054 completed.

3055
3056 c. Public Release of Automatically Declassified Documents. Automatic declassification does
3057 not constitute approval for public release of the information. Automatically declassified documents
3058 shall not be released to the public until a public disclosure review has been conducted in accordance
3059 with paragraph 1.e. of this enclosure. Declassified information may be designated CUI in
3060 accordance with Volume 4 of this Manual if it meets the criteria for designation; information so
3061 designated shall be marked and protected as Volume 4 requires.

3062
3063 d. Basis for Exclusion or Exemption from Automatic Declassification. Information shall be
3064 excluded or exempted from automatic declassification provisions based on content. Exclusion or
3065 exemption shall not be based solely on the type of document or record in which the information is
3066 found.

3067
3068 e. Exclusion of RD and FRD. Documents and other materials marked or containing RD or
3069 FRD are excluded from the automatic declassification provisions of Reference (d) and this Volume
3070 until the RD or FRD designation is properly removed. Such information shall remain classified or
3071 shall be referred for a declassification review to the DOE if RD or the DASD(NM) if FRD.

3072
3073 (1) In accordance with the provisions of section 3161 of Public Law 105-261 (Reference
3074 (bg) (also known as “The Kyl-Lott Amendment”), and its implementing plan, all personnel who
3075 perform automatic declassification reviews on records that are highly likely to contain RD or FRD
3076 must be trained and certified by the DOE in the identification of unmarked RD and FRD
3077 information. DoD Components shall report each confirmed inadvertent release of RD or FRD
3078 occurring during declassification processes to the DOE and provide a copy to the USD(I&S)
3079 Security Directorate.

3080
3081 (2) When the RD or FRD pertains to defense nuclear information, declassification reviews
3082 shall be referred to the DASD(NM), who has OCA for defense nuclear information, to include joint
3083 OCA with the DOE for FRD.

3084
3085 (3) The Secretary of Energy determines when information concerning foreign nuclear
3086 programs that was removed from the RD category in order to carry out provisions of section 2673
3087 of Reference (DAF) may be declassified. Unless otherwise determined by the appropriate OCA,
3088 such information shall be declassified when comparable information concerning the U.S. nuclear
3089 program is declassified.

3090
3091 f. Integral File Block. Classified records within an integral file block that are otherwise
3092 subject to automatic declassification in accordance with this section shall not be automatically
3093 declassified until December 31 of the year that is 25 years from the date of the MOST RECENT

3094 record or the date specified by the exemption instruction of the most recent exempted record,
 3095 whichever is later, within the file block. For purposes of automatic declassification, integral file
 3096 blocks shall contain only records dated within 10 years of the oldest record in the file block.

3097
 3098 g. Delays of Automatic Declassification. The following lists the scenarios for which
 3099 automatic declassification may be delayed.

3100
 3101 (1) Media That Is Difficult or Costly to Review. Before the records are subject to
 3102 automatic declassification, a DoD Component Head or senior agency official may delay automatic
 3103 declassification for up to 5 additional years for classified information contained in media that make
 3104 a review for possible declassification more difficult or costly. Prior to taking such action, officials
 3105 shall consult with the NDC Director, either through the Component declassification plan or by
 3106 memorandum. The Heads of the Military Departments or their senior agency official shall consult
 3107 with the NDC Director directly and provide an information copy to the USD(I&S). Other DoD
 3108 Component Heads or their senior agency official shall consult with the NDC Director through
 3109 USD(I&S).

3110
 3111 (a) When determined by NARA or jointly determined by NARA and the DoD,
 3112 automatic declassification may be delayed for:

3113
 3114 1. Records requiring extraordinary preservation or conservation treatment, to
 3115 include reformatting, to preclude damage to the records by declassification processing.

3116
 3117 2. Records that pose a potential menace to health, life, or property due to
 3118 contamination by a hazardous substance.

3119
 3120 3. Electronic media if the media is subject to issues of software or hardware
 3121 obsolescence or degraded data.

3122
 3123 (b) Information contained in such media that has been referred shall be automatically
 3124 declassified five (5) years from the date of notification or 30 years from the date of origination of
 3125 the media, whichever is longer, unless the information has been properly exempted.

3126
 3127 (2) Newly Discovered Records. The Director, ISOO, must be consulted whenever a DoD
 3128 Component Head determines there is a need to delay automatic declassification for newly
 3129 discovered records that were inadvertently not reviewed prior to the effective date of automatic
 3130 declassification. Such consultation shall occur not later than 90 days from discovery of the records.
 3131 Heads of the Military Departments or their senior agency official will notify ISOO directly and
 3132 provide an information copy to USD(I&S). Other DoD Component Heads or their senior agency
 3133 official will notify ISOO through the USD(I&S). The notification should identify the records and
 3134 their volume, explain the circumstances leading to discovery of the missed records, and provide the
 3135 anticipated date for declassification. A DoD Component has up to 3 years from the date of
 3136 discovery to make a declassification, exemption, or referral determination. Referral to other DoD
 3137 Components or Federal entities with identified interests or equities shall be in accordance with
 3138 subparagraph 12.g.(3) and section 15 of this enclosure.

3139
 3140 (3) Referred Records

3141
 3142 (a) Referring Other Agency Information. Other than records that are properly

...

3143 excluded or exempted from automatic declassification, records containing classified information
3144 originated by another department or agency or the disclosure of which would affect the interests or
3145 activities of other departments or agencies with respect to the classified information and that could
3146 reasonably be expected to fall under one or more of the exemptions identified in paragraph 13.b. of
3147 this enclosure shall be identified prior to onset of automatic declassification for later referral to
3148 those departments or agencies. DoD Components shall identify other agency information for
3149 referral during the initial review of Component records; referral review will take place under the
3150 auspices of the NDC. The records shall be referred using SF 715, "U.S. Government
3151 Declassification Review Tab."

3152
3153 (b) Referrals to the Department of Defense. Other agency records subject to
3154 automatic declassification that contain defense information shall be reviewed by the appropriate
3155 DoD Component upon referral. If a final determination is not provided within one (1) year on a
3156 referral made by the NDC, defense information in the referred records shall be automatically
3157 declassified.

3158
3159 (c) DoD Component Referrals to Other DoD Components. Records containing
3160 information originated by another DoD Component or the disclosure of which would affect the
3161 interests or activities of another DoD Component with respect to the classified information shall
3162 be referred and processed through the NDC, as appropriate. The DoD Component shall be
3163 notified of these types of referrals.

3164
3165 (d) Referral Review Period. If any disagreement arises between a DoD Component
3166 and the NDC regarding the referral review period, the DoD Component shall notify ISOO and
3167 USD(I&S) of the disagreement. In such cases, the Director of ISOO shall determine the
3168 appropriate review period for referred records. Otherwise, the DoD Component shall provide a
3169 final determination on referrals received through the NDC within one (1) year of referral or the
3170 information shall be automatically declassified. If any disagreement arises among the DoD
3171 Components regarding the referral review period, the USD(I&S), shall determine the
3172 appropriate period of review for the referred records.

3173
3174 h. Automatic Declassification of Backlogged Records at NARA. In accordance
3175 with Presidential Memorandum (Reference (bh)) and under NDC direction:

3176
3177 (1) Referrals and quality assurance problems within the backlog of more than 400
3178 million pages of accessioned Federal records previously subject to automatic declassification
3179 shall be addressed in a manner that will permit public access to all declassified records from this
3180 backlog no later than December 31, 2013.

3181
3182 (2) DoD Components shall review all referrals to DoD in the backlogged records and
3183 identify potentially exemptible information for further referral to other agencies. For DoD, the
3184 backlog includes all records reviewed for automatic declassification from April 1995 to
3185 December 2009 that have been accessioned, but not processed, by NARA.

3186
3187 i. Declassification Review Technique. DoD Components may use a pass/fail or a
3188 redaction declassification technique when doing automatic declassification reviews.

3189
3190
3191 13. EXEMPTIONS FROM AUTOMATIC DECLASSIFICATION. Reference (d) sets out three

types of exemptions, specific criteria and duration, and the requirements for requesting an exemption from automatic declassification. Information not exempted from automatic declassification shall be automatically declassified no later than December 31 of the year that is 25 years from the date of origin. Information exempted from automatic declassification remains subject to the mandatory and systematic declassification review provisions of this Volume.

a. Exemption Types

(1) Specific Information. This exemption option permits OCAs to identify and select specific information that should be exempted from the automatic declassification provisions. The information is described topically in a manner similar to how topics of information are described in a security classification guide and must fall within one or more of the exemption categories described in paragraph 13.b. of this section.

(2) Specific Records. This exemption option permits OCAs to identify and select specific records for exemption from the automatic declassification provisions. The records must be described at the records title level and must contain information that is eligible for exemption under one or more of the exemption categories described in paragraph 13.b. of this section.

(3) File Series. This exemption option allows OCAs to identify an entire file series that should be exempted from the automatic declassification provisions. File series shall be considered for exemption only after a review or assessment has determined that the series is replete with information that almost invariably falls within one or more of the exemption categories described in paragraph 13.b. of this section.

b. Exemption Criteria and Duration

(1) Exempting 25-Year-Old Information. Information that is 25 years old may be exempted (by topic or file series) from automatic declassification for a period not to exceed 50 years from the date of origin when the release would clearly and demonstrably be expected to:

(a) Reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development (exemption 25X1);

(b) Reveal information that would assist in the development, production, or use of weapons of mass destruction (exemption 25X2);

(c) Reveal information that would impair U.S. cryptologic systems or activities (exemption 25X3);

(d) Reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system (exemption 25X4);

(e) Reveal formally named or numbered U.S. Military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans (exemption 25X5);

3241 (f) Reveal information, including FGI, that would cause serious harm to relations
3242 between the United States and a foreign government, or to ongoing diplomatic activities of the
3243 U.S. (exemption 25X6);
3244

3245 (g) Reveal information that would impair the current ability of U.S. Government
3246 officials to protect the President, Vice President, and other protectees for whom protection
3247 services, in the interest of the national security, are authorized (exemption 25X7);
3248

3249 (h) Reveal information that would seriously impair current national security
3250 emergency preparedness plans or reveal current vulnerabilities of systems, installations, or
3251 infrastructures relating to the national security (exemption 25X8); or
3252

3253 (i) Violate a statute, treaty, or international agreement that does not permit the
3254 automatic or unilateral declassification of information at 25 years (exemption 25X9).
3255

3256 (2) Exempting 50-Year-Old Information. Information that is 50 years old may continue
3257 to be exempted (by topic or files series) from automatic declassification for an additional 25
3258 years (i.e., for a period not to exceed 75 years from the date of origin) when:
3259

3260 (a) The release would clearly and demonstrably be expected to reveal the identity of
3261 a confidential human source or a human intelligence source (exemption 50X1-HUM), or key
3262 design concepts of weapons of mass destruction (exemption 50X2-WMD), or
3263

3264 (b) In extraordinary cases, the Secretary of Defense or the Secretary of a Military
3265 Department, or their senior agency officials, as appropriate, proposes within five (5) years of
3266 the onset of automatic declassification to further exempt specific information from
3267 declassification at 50 years. The exemption category numbers are the same as for 25 year
3268 exemptions, except the number "50" shall be used in place of "25."
3269

3270 (3) Exempting 75-Year-Old Information. The Secretary of Defense or the Secretaries of
3271 the Military Departments, or their senior agency officials, as appropriate, may propose within
3272 five (5) years of the onset of automatic declassification to further exempt specific information
3273 from declassification at 75 years. Such proposals must be formally accepted by the ISCAP.
3274 The exemption category numbers are the same as for 25 year exemptions, except the number
3275 "75" shall be used in place of "25."
3276

3277 (4) File Series Exemptions Approved Prior to December 31, 2008. File series
3278 exemptions approved by the President prior to December 31, 2008, shall remain valid without
3279 any additional DoD Component action pending ISCAP review by the later of December 31,
3280 2010, or December 31 of the year that is 10 years from the date of previous approval.
3281

3282 (5) Declassification of 50-Year-Old Information in Previously Exempted Records. All
3283 previously exempted records, both file series and specific information, that are 50 years or older
3284 as of December 31, 2012, shall be automatically declassified by that date unless further
3285 exempted in accordance with subparagraphs 13.b.(2) through 13.b.(4) of this section. All
3286 existing records meeting the criteria shall be processed for declassification by December 31,
3287 2012. Declassification actions shall be accomplished in accordance with the schedule and
3288 priority issued by the NDC. After December 31, 2012, previously exempted records shall be
3289 automatically declassified on December 31 of the year that is no more than 50 years from the

3290 date of origin unless further exempted in accordance with this section.

3291
3292 c. Exemption Requests. Requests for exemption shall include all information necessary
3293 for making a decision. Requests to extend the duration of an exemption shall be processed in
3294 the same manner as an initial request.

3295
3296 (1) Requesting an Exemption for Specific Information or Specific Records. OCAs shall
3297 provide the following information:

3298 (a) A detailed description of the information, in the form of a declassification guide.

3299
3300 (b) An explanation of why the information should be exempt from automatic
3301 declassification and must remain classified for a longer period of time.

3302
3303 (c) A specific date or a specific and independently verifiable event for automatic
3304 declassification of specific records that contain the information proposed for exemption. The
3305 date or event shall not exceed December 31 of the year that is 50 years from the date of origin of
3306 the records (75 years for 50 year old material), except a date or event is not required when the
3307 information identifies a confidential human source or a human intelligence source or key design
3308 concepts of weapons of mass destruction.

3309
3310 (d) If appropriate, a statement that the exemption will be cited subsequently in
3311 applicable classification guides to provide declassification guidance.

3312
3313 (e) If requesting an exemption from declassification at 50 or 75 years, a statement of
3314 support from the USD(I&S), as the designee of the Secretary of Defense. DoD Components that
3315 are elements of the Intelligence Community shall also provide a statement of support from the
3316 DNI.

3317
3318 (2) Requesting an Exemption for a File Series. OCAs shall provide the following
3319 information:

3320 (a) A description of the file series.

3321
3322 (b) An explanation of why the information within the file series is almost invariably
3323 exempt from automatic declassification and why the information must remain classified for a
3324 longer period of time.

3325
3326 (c) A specific date or event for declassification of the information, not to exceed
3327 December 31 of the year that is 50 years from the date of origin of the records (75 years for 50
3328 year old information), except a date or event is not required when the information within the file
3329 series almost invariably identifies a confidential human source or a human intelligence source or
3330 key design concepts of weapons of mass destruction.

3331
3332 (d) If appropriate, a statement that the exemption will be cited subsequently in
3333 applicable classification guides to provide declassification guidance.

3334
3335 (e) If requesting an exemption from declassification at 50 or 75 years, a statement of
3336 support from the USD(I&S), as the designee of Secretary of Defense. DoD Components that

3339 are elements of the Intelligence Community shall also provide a statement of support from the
3340 DNI.

3341
3342 d. When to Request an Exemption. Exemptions shall be requested not more than five (5)
3343 years and not less than one (1) year before information is subject to automatic declassification
3344 except for 75-year exemptions which shall be requested in accordance with subparagraph
3345 13.b.(3) of this section.

3346
3347 e. Who Identifies and Requests an Exemption. In all cases, OCAs are responsible for
3348 identifying information that should be exempted from automatic declassification. The type of
3349 exemption requested (i.e., specific information, specific records, or file series) determines who
3350 must request the exemption.

3351
3352 (1) Specific Information and Specific Records. The SAO of a Military Department or
3353 the USD(I&S) acting as the DoD senior agency official, as appropriate, requests exemptions for
3354 specific information and specific records from automatic declassification. OCAs, except those in
3355 a Military Department, shall request exemptions for specific information and specific records
3356 through their DoD Component Head to USD(I&S). USD(I&S) shall notify the Director of
3357 ISOO, serving as Executive Secretary of the ISCAP, of any information or records that the
3358 Component proposes to exempt from automatic declassification. OCAs within a Military
3359 Department shall request exemptions through their Department's senior agency official, who
3360 shall notify the Director of ISOO and provide USD(I&S) an information copy for oversight
3361 purposes.

3362
3363 (2) File Series. For file series exemptions, the Secretary of Defense or the Secretary of a
3364 Military Department, as appropriate, must request the exemption. In either case, the request is
3365 forwarded to the Director of ISOO, serving as Executive Secretary of the ISCAP. OCAs, except
3366 those within a Military Department, shall submit requests for file series exemption through their
3367 DoD Component Head to USD(I&S). USD(I&S) will forward the request to the Secretary of
3368 Defense for decision and ISCAP notification. OCAs within the Military Departments shall
3369 submit requests for exemption to the Secretary of the Military Department, who shall notify the
3370 ISCAP. Military Departments shall provide USD(I&S) an information copy of such
3371 notifications for oversight purposes.

3372
3373 f. ISCAP Authority. The ISCAP may direct the Department of Defense not to exempt the
3374 specific information, specific records, or file series, or to declassify it at an earlier date than
3375 recommended. The Secretary of Defense or the Secretary of a Military Department, as
3376 appropriate, may appeal such a decision to the President through the National Security
3377 Advisor. The information will remain classified while such an appeal is pending. OCAs shall
3378 notify the appropriate DoD authority if an appeal is necessary and provide justification and
3379 rationale to counter the ISCAP decision. Military Departments shall provide USD(I&S) an
3380 information copy of any appeal for oversight purposes.

3381
3382 g. Notice to Information Holders. When information has been approved for exemption by
3383 the ISCAP, the OCA must notify all known information holders. This may be done through
3384 issuance of a memorandum or distribution of the declassification guide. DoD Components that
3385 have ISCAP-approved declassification guides must ensure maximum dissemination to record
3386 holders of the information. Holders shall re-mark documents in their possession to reflect the
3387 exemption.

3388
3389
3390 14. DECLASSIFICATION OF INFORMATION MARKED WITH OLD DECLASSIFICATION
3391 INSTRUCTIONS

3393 a. In accordance with Reference (f), when information is marked with previously authorized
3394 exemption categories X-1 through X-8, or with the instructions “OADR” (Originating Agency’s
3395 Determination Required) or “MR” (Manual Review), including when preceded by “Source
3396 marked,” use a declassification date of 25 years from the date of the source document or 25 years
3397 from the current date if the source document date is not available, unless exempted in accordance
3398 with section 13 of this enclosure.

3399
3400 b. If imagery subject to E.O. 12951 (Reference (bi)) is marked with the declassification
3401 instruction “DCI Only” or “DNI Only,” use “25X1, E.O. 12951” as the declassification
3402 instruction, as specified by the DNI (Contact the National Geospatial-Intelligence Agency,
3403 Classification Management (NGA/SISX) for assistance in determining whether specific imagery
3404 is subject to E.O. 12951). Otherwise, for documents marked with the declassification
3405 instructions “DCI Only” or “DNI Only” which do NOT contain information subject to Reference
3406 (bi), use a declassification date that is 25 years from the date of the source document or 25 years
3407 from the current date if the source document date is not available.

3408
3409
3410 15. REFERRALS IN THE AUTOMATIC DECLASSIFICATION PROCESS. Referrals are
3411 required by References (d) and (f) to ensure timely, efficient, and effective processing of reviews
3412 and to protect classified information from inadvertent disclosure. All referrals contained within
3413 accessioned records will be processed through the NDC.

3414
3415 a. Description. The referral process involves identification of information in records
3416 containing classified information that originated with another DoD Component or Executive
3417 Branch agency or the disclosure of which would affect the interests or activities of another DoD
3418 Component or Executive Branch agency and that could reasonably be expected to fall within one
3419 or more of the exemptions listed in subparagraph 13.b.(1) of this enclosure. Such records are
3420 eligible for referral. The referral process also requires formal notification of referral, making the
3421 records available for review, and recording final determinations.

3422
3423 b. Referral Responsibility. Identification of records eligible for referral is the responsibility
3424 of the primary reviewing agency and shall be completed prior to the date for automatic
3425 declassification established in accordance with section 12 of this enclosure. DoD Components
3426 shall use SF 715 to identify any record requiring referral.

3427
3428
3429 16. MANDATORY DECLASSIFICATION REVIEW. Any individual or organization may
3430 request a declassification review of information classified pursuant to Reference (d) or previous
3431 classified national security information orders. Heads of the DoD Components shall establish
3432 processes for responding to such requests in accordance with Reference (f).

3433
3434 a. Information reviewed shall be declassified if it no longer meets the standards for
3435 classification established by this Volume. The declassified information shall be released unless
3436 withholding is authorized under other applicable law and the requirement of paragraph 1.e. of

3437 this enclosure.

3438
3439 b. Upon receiving a request for a mandatory declassification review, the responsible DoD
3440 organization shall conduct the review if:

3441
3442 (1) The request describes the document or material with enough specificity to allow DoD
3443 Component personnel to locate the records with a reasonable amount of effort. Requests for
3444 broad types of information, entire file series of records, or similar non-specific requests may be
3445 denied.

3446
3447 (2) The information falls under its purview.

3448
3449 (a) If documents or material being reviewed for declassification contain information
3450 originally classified by another DoD Component or U.S. Government agency or the disclosure of
3451 which would affect the interests or activities of another DoD Component or U.S. Government
3452 agency, the reviewing activity shall refer the appropriate portions of the request to the originating
3453 or affected organization. Unless the association of that organization with the requested
3454 information is itself classified, the DoD Component that received the review request shall notify
3455 the requester of the referral. The DoD Component that received the review request remains
3456 responsible for collecting all determinations made by organizations to which the information was
3457 referred and for informing the requestor of the final decision regarding declassification, unless
3458 other prior arrangements have been made.

3459
3460 (b) Requests for cryptologic information shall be processed in accordance with
3461 section 7 of this enclosure.

3462
3463 (c) The DoD Component that initially received or classified FGI shall determine
3464 whether the information is subject to a treaty or international agreement that does not permit
3465 unilateral declassification (Refer also to section 20 of this enclosure).

3466
3467 (3) The information is not the subject of pending litigation.

3468
3469 (4) The information is not contained within an operational file that is exempt from search
3470 and review, or disclosure, pursuant to sections 3141, 3142, 3143 and 3144 of Reference (DAF)
3471 or other applicable statute.

3472
3473 (5) The information has not been reviewed for declassification within the preceding two
3474 (2) years. If the requested information has been reviewed for declassification within the two (2) years
3475 preceding the request, the DoD Component shall notify the requester of the prior review decision and
3476 provide appeal rights information. No further review is required.

3477
3478 (6) The information was not originated by the incumbent President or the incumbent
3479 Vice President, the incumbent President's White House staff, or the incumbent Vice President's
3480 staff, committees, commissions, or boards appointed by the incumbent President, or other entities
3481 within the Executive Office of the President that solely advise and assist the incumbent
3482 President. Information so originated is exempt from the provisions of this section.

3483
3484 (7) The request was submitted to a Defense Intelligence Component by a U.S. citizen or
3485 an alien lawfully admitted for permanent residence; otherwise, the request may be denied.

3486
3487 c. A DoD Component may refuse to confirm or deny the existence or nonexistence of
3488 requested information when the fact of its existence or nonexistence is properly classified.

3489
3490 d. DoD Components shall either make a prompt declassification determination and notify the
3491 requester accordingly, or inform the requester of the additional time needed to process the
3492 request. DoD Components shall ordinarily make a final determination within one (1) year from
3493 the date of receipt.

3494
3495 (1) In making a declassification determination DoD Components shall determine
3496 whether the information continues to meet the requirements for classification. Information to be
3497 withheld must not only qualify for classification under the criteria identified in paragraph 1.b of
3498 Enclosure 4, but there also must be a current basis for continued classification.

3499
3500 (2) When information cannot be declassified in its entirety, DoD Components shall make
3501 reasonable efforts to release, consistent with other applicable law and the requirements of
3502 paragraph 1.e. of this enclosure, those declassified portions of the requested information that
3503 constitute a coherent segment. Where information is withheld the specific reason, as specified
3504 by section 1.4 of Reference (d) and identified in paragraph 1.b of Enclosure 4 of this Volume,
3505 must be included for each redaction. Information that is redacted due to a statutory authority
3506 must be clearly marked with the specific authority that authorizes the redaction.

3507
3508 e. The mandatory declassification review process shall provide for administrative appeal in
3509 cases where the review results in the information remaining classified. The requester shall be
3510 notified of the results of the review and of the right to appeal, within 60 days of receipt, the
3511 denial of declassification. If the requester files an appeal, the DoD Component appellate
3512 authority shall make a determination within 60 working days following receipt. If additional
3513 time is required to make a determination, the appellate authority shall notify the requestor of
3514 the additional time needed and provide the reason for the extension. If the appeal is denied, the
3515 requester shall be notified of the right to appeal the denial to the ISCAP.

3516
3517 f. Requesters may be charged fees for processing their requests in accordance with the
3518 schedule of fees in Volume 11A of DoD 7000.14-R (Reference (bj)).

3519
3520 **g. (Added)(DAF) SAF/AII oversees the DAF MDR program. SAF/AII will:**

3521
3522 **(1) (Added)(DAF) Determine if the request provides enough specificity to allow**
3523 **the field OPR to locate the records, with a reasonable amount of effort. If not, deny the**
3524 **request.**

3525
3526 **(2) (Added)(DAF) Provide written acknowledgment to the requester, no later**
3527 **than 24 hours after receiving the request.**

3528
3529 **(3) (Added)(DAF) Ensure each request is logged into the database.**

3530
3531 **(4) (Added)(DAF) Control and process MDR requests through completion.**

3532
3533 **(5) *(Added)(DAF) Review the DAF declassification manual (controlled by AFDO)**
3534 **and determine if the information is over 25 years old, has already been declassified, or has**

...

3535 an exemption from declassification. If information is less than 25 years old, has not already
3536 been declassified, and does not have an exemption from declassification, refer the request
3537 to the appropriate field OPR. If the information is older than 25 years old, refer the
3538 request to AFDO.

3539
3540 (6) (Added)(DAF) Establish procedures to assess and collect fees; approve or deny
3541 fee waivers; and, notify requester, in writing, of possible MDR fees.

3542
3543 (7) (Added)(DAF) Send extension notices to requester.

3544
3545 (8) (Added)(DAF) Notify requester of the right of an administrative appeal when
3546 information is denied in full or in part.

3547
3548 (9) (Added)(DAF) Make final determination on all “no records” responses.

3549
3550 (10) *(Added)(DAF) Contact MAJCOM/FLDCOM MDR monitors and schedule
3551 training within 15 days of an individual receiving his/her appointment letter. At minimum,
3552 the training will consist of determining equities or ownership of information contained in a
3553 document or electronic form.

3554
3555 (11) (Added)(DAF) MAJCOM/FLDCOM MDR monitors will:

3556
3557 (a) (Added)(DAF) Work closely with SAF/AII to ensure MDR requests are
3558 properly processed, meet prescribed timelines, and serve as the liaison between the
3559 MAJCOM/FLDCOM OPR and SAF/AII. (T-1).

3560
3561 (b) (Added)(DAF) Contact SAF/AII within 15 days of appointment and
3562 complete all training requirements, in accordance with SAF/AII processes. (T-1).

3563
3564 (c) *(Added)(DAF) Determine MAJCOM/FLDCOM OPR (or stakeholders)
3565 with equity and staff request accordingly. (T-1).

3566
3567 (d) (Added)(DAF) Process the release or denial with SAF/AII office. (T-1).

3568
3569 (e) (Added)(DAF) Submit requests for extensions 60 days prior of the 1-year
3570 suspense (at minimum). (T-1).

3571
3572 (f) (Added)(DAF) Respond to set timelines for interim updates on progress.
3573 (T-1).

3574
3575 (g) (Added)(DAF) Notify SAF/AII of the following occurrences, at
3576 minimum. (T-1).

3577
3578 1. (Added)(DAF) A requester is denied information.

3579
3580 2. (Added)(DAF) An external agency’s equities are involved, to ensure
3581 proper coordination with the appropriate stakeholders.

3582
3583 3. (Added)(DAF) When unable to make a determination because the

3584 OCA, or originating OPR, of the classified information no longer exists.

3585
3586 **4. (Added)(DAF) The functions of the originating OCA, or originating**
3587 **OPR, were dispersed to more than one organization.**

3588
3589 **5. (Added)(DAF) Inheriting OCA cannot be determined.**

3590
3591 **6. (Added)(DAF) The document is lacking markings to indicate what**
3592 **information is classified.**

3593
3594 **(h) (Added)(DAF) Upon receipt of the MDR, monitors shall:**

3595
3596 **1. (Added)(DAF) Use brackets to identify the classified information,**
3597 **and cite the applicable exemption, in the margins closest to the bracketed information.**
3598 **(T-1).**

3599
3600 **2. (Added)(DAF) Use brackets to identify the CUI that is not releasable**
3601 **and cite the applicable CUI category(ies), in the margins closest to the bracketed**
3602 **information. (T-1).**

3603
3604 **(i) *(Added)(DAF) Initial Denial Authority (IDA). The IDA is a reviewer who**
3605 **has authority to deny requested information, consistent with DoDM 5400.07_AFMAN 33-**
3606 **302, *Freedom of Information Act Program*. At the HAF/SAF level, the IDA must be a GS-**
3607 **15/O-6, or above. Outside the HAF/SAF level, commanders and vice commanders will**
3608 **appoint the IDA. (T-1). The IDA must be a GS-13/O-4, or above. The IDA shall:**

3609
3610 **1. (Added)(DAF) Review all classified information and determine if any**
3611 **of the classified information has been declassified. (T-1).**

3612
3613 **2. (Added)(DAF) If MDR contains CUI, determine if it is releasable.**
3614 **(T-1).**

3615
3616 **3. (Added)(DAF) Deny release of any information that remains**
3617 **classified or any declassified information that falls under a CUI category(ies). (T-1).**

3618
3619 **4. (Added)(DAF) Approve release of all unclassified information, not**
3620 **protected by a CUI category(ies). (T-1).**

3621
3622 **5. (Added)(DAF) Submit the final determination to the MDR monitor.**
3623 **Include one or more of the exemptions identified in paragraph 13 of this volume that apply**
3624 **to denial of release for the classified information; and, list the CUI category(ies) that apply**
3625 **to the denial of release for the unclassified information. (T-1).**

3626
3627
3628 **17. SYSTEMATIC REVIEW FOR DECLASSIFICATION. Heads of the DoD Components that**
3629 **have classified information in accordance with Reference (d) or previous Executive orders shall**
3630 **establish systematic review programs to review for declassification information in the custody of**
3631 **the DoD Component. These programs shall review for declassification information that is**
3632 **contained in permanently valuable historical records that have been exempted from automatic**

3633 declassification and shall determine if the information may be further exempt from automatic
3634 declassification in accordance with the provisions of this enclosure. These efforts shall be
3635 prioritized in accordance with the priorities established by the NDC.

3636
3637
3638 18. DOWNGRADING CLASSIFIED INFORMATION. Downgrading information to a lower
3639 level of classification is appropriate when the information no longer requires protection at the
3640 originally assigned level and can be properly protected at a lower level. The principal purpose of
3641 downgrading is to conserve security resources by avoiding protection of information at too high a
3642 level. Any official with jurisdiction over the information who is authorized to classify or
3643 declassify the information may downgrade it.

3644
3645 a. Downgrading shall be considered when OCAs are deciding on the duration of classification
3646 to be assigned. If downgrading dates or events can be identified, they shall be specified along with
3647 the declassification instruction. Downgrading instructions do not replace declassification
3648 instructions.

3649
3650 b. An authorized official making a downgrading decision shall notify all known holders of the
3651 change in classification. If the information is subject to the Scientific and Technical Information
3652 Program (STIP) (DoDD 3200.12 (Reference (bk))), the authorized official shall also notify DTIC.

3653
3654 c. When information is marked for downgrading on a specific date or event and that date or
3655 event has passed, holders shall confirm that the OCA(s) of the information has not extended the
3656 higher classification period prior to downgrading DoD information.

3657
3658 d. Downgraded information shall be marked, as required by Enclosure 3 of Volume 2 of this
3659 Manual.

3660
3661 e. If a holder of classified information has reason to believe it should not be downgraded as
3662 indicated, the originator shall be notified through appropriate administrative channels. The
3663 document or material shall continue to be protected at the originally assigned classification until
3664 the issue is resolved.

3665
3666
3667 19. UPGRADING CLASSIFIED INFORMATION. Classified information may be upgraded to
3668 a higher level of classification only by officials who have been delegated the appropriate level of
3669 OCA in accordance with Enclosure 4 of this Volume. The information to be upgraded must
3670 continue to meet the standards for classification specified in Enclosure 4 of this Volume. When
3671 making the decision to upgrade the classification level, OCAs shall consider the benefits to
3672 national security that will accrue from the higher classification against the costs associated with
3673 upgrading (e.g., the requirement for upgraded clearances or storage facilities, notification costs)
3674 and the ability to notify all holders of the information of the change so that the information shall
3675 be uniformly protected at the higher level. The OCA making the upgrading decision is
3676 responsible for notifying holders of the change in classification. For information subject to the
3677 STIP (Reference (bk)), the OCA shall also notify DTIC. Upgraded information shall be marked
3678 as required by Enclosure 3 of Volume 2 of this Manual.

3679
3680
3681 20. DECLASSIFYING FGI. Pursuant to Reference (d), FGI qualifies as an exemption to the

3682 automatic declassification rule. Within the DoD, every effort shall be made to ensure that FGI is
3683 not subject to downgrading or declassification without the prior consent of the originating
3684 government. FGI may exist in two forms: foreign documents in possession of the DoD, and
3685 foreign government classified information included within U.S. Government documents.

3686
3687 a. If FGI in the form of foreign documents in the possession of the DoD constitute
3688 permanently valuable records of the U.S. Government and are subject to the 25-year automatic
3689 declassification rule, declassification officials shall consult with the originating foreign
3690 government to determine whether it consents to declassification. If the originating foreign
3691 government does not consent, the records shall be processed for exemption from automatic
3692 declassification in accordance with section 13 of this enclosure. The agency head shall
3693 determine whether exemption category 25X6, 25X9, or both, should be applied.

3694
3695 b. U.S. Government documents that include classified FGI shall be marked with
3696 declassification instructions as specified in this enclosure and Volume 2 of this Manual. If these
3697 documents are permanently valuable records of the U.S. Government and are subject to the 25-
3698 year automatic declassification rule, the provisions of paragraph 20.a. of this section shall apply.
3699 A U.S. document marked as described herein cannot be downgraded below the highest level of
3700 FGI contained in the document or be declassified without the written permission of the foreign
3701 government or international organization that originated the information. Submit
3702 recommendations concerning downgrading or declassification to the DoD organization that
3703 created the document. If that organization supports the recommendation, it shall consult with
3704 the originating foreign government to determine whether that government consents to
3705 declassification.

3706
3707 c. DoD officials may consult directly with foreign governments regarding downgrading or
3708 declassification of FGI or seek assistance from the Department of State. In either case, DoD
3709 officials should first consult with the Director, International Security Programs, Defense
3710 Technology Security Administration, USD(P), for assistance and guidance.

3711
3712
3713 **21. APPLICATION OF DECLASSIFICATION AND EXTENSION OF CLASSIFICATION**
3714 **TO PRESENT AND PREDECESSOR EXECUTIVE ORDERS.** The requirements for
3715 declassifying and extending classification specified by this enclosure apply to information
3716 classified in accordance with E.O. 12958 (Reference (b)) and earlier E.O., as well as to
3717 information classified pursuant to Reference (d).
3718

...

ENCLOSURE 6

SECURITY CLASSIFICATION GUIDES

3719
3720
3721
3722
3723
3724
3725 1. GENERAL. Reference (d) requires issuance of classification guidance to facilitate proper and
3726 uniform derivative classification of information. Issuance of timely and precise classification
3727 guidance by the responsible OCA is a prerequisite to effective and efficient information security
3728 and assures that security resources are expended to protect only that information warranting
3729 protection in the interests of national security.

3730
3731 a. The responsible OCA shall issue a security classification guide (SCG) for each system,
3732 plan, program, or project involving classified information as early as practical and in accordance
3733 with DoDM 5200.45 (Reference (bm), which provides guidance to assist in development of the
3734 SCG as well as identifying the mandatory format.

3735
3736 b. Prior to signing the SCG, OCAs must communicate with other stakeholders responsible for
3737 SCGs on similar systems, plans, programs, or projects to ensure consistency and uniformity of
3738 classification decisions. This is accomplished by conducting a review of other SCGs on the DTIC
3739 portal, or by reviewing other known SCGs not housed on the DTIC portal. Additionally, when
3740 possible OCAs should seek user input when reviewing guides for revision.

3741
3742 c. The OCA must ensure SCGs are reviewed at each milestone and updated to ensure
3743 protection measures are adequate for critical program information, critical components, and CUI.

3744
3745 d. If the-SCG does not meet the requirements to be classified, at a minimum, it should be
3746 marked and protected in accordance with DoDI 5200.48, as a category of CUI. SCGs shall not be
3747 released to the public nor posted on publicly accessible websites.

3748
3749 e. OCAs must comply with the mandatory five (5) year review and reporting requirements for
3750 SCGs prescribed by ISOO.

3751
3752 **f. *(Added)(DAF) At the time of the 5 year review, if the SCG does not require any**
3753 **substantive changes, at minimum, a properly filled out DD Form 2024 will be submitted to**
3754 **DTIC. (T-0). Along with the DD Form 2024, submit a copy of the SCG, with the updated**
3755 **revision date on the cover page. (T-0).**

3756
3757
3758 2. CONTENT OF SECURITY CLASSIFICATION GUIDES. Security classification guides
3759 shall:

3760 a. Identify specific items or elements of information to be protected.

3761
3762 b. State the specific classification assigned to each item or element of information. Where an
3763 item or element of information may qualify for one of multiple classification levels, criteria must be
3764 provided for determining which classification level is applicable, in the remarks column of the
3765 SCG. Simply citing a range is not permissible.

3766
3767 c. State a concise reason for classifying each item, element, or category of information and
3768

3769 cite the applicable classification category(ies) in section 1.4 of Reference (d).

3770
3771 d. State the declassification instructions for each item or element of classified information,
3772 including citation of the approved automatic declassification exemption category, if any.

3773
3774 (1) For information exempted from automatic declassification because disclosing it may
3775 reveal FGI or violate a statute, treaty, or international agreement (see subparagraphs 13.b.(1)(f) and
3776 13.b.(1)(i) of Enclosure 5 of this Volume), the guide shall identify the government or specify the
3777 applicable statute, treaty, or international agreement as appropriate.

3778
3779 (2) Automatic declassification exemptions (25X1 – 25X9) authorized in accordance with
3780 section 13 of Enclosure 5 of this Volume may be cited in the SCG for use on derivatively classified
3781 documents once the declassification guide has been submitted to the ISCAP. The ISCAP must be
3782 notified in advance of the declassification guide's approval of the intent to cite such exemptions in
3783 applicable SCGs (refer to paragraph 13.c. of Enclosure 5 of this Volume), and the information
3784 being exempted must remain in active use.

3785
3786 (3) Where applicable, the SCG should refer to the declassification guide for specific
3787 declassification guidance.

3788
3789 e. Identify any special handling caveats (e.g., dissemination controls) that apply to items,
3790 elements, or categories of information. Where applicable, use remarks or an annex to identify those
3791 elements of information approved, in accordance with established disclosure policies, by the
3792 appropriate disclosure authority(s) for routine release to specified foreign governments and
3793 international organizations.

3794
3795 f. Identify, by name or personal identifier and position title, the OCA approving the SCG and
3796 the date of approval.

3797
3798 g. Provide a point of contact for questions about the guide and suggestions for improvement.

3799
3800
3801 3. CUI AND UNCLASSIFIED ELEMENTS OF INFORMATION. OCAs and developers of
3802 SCGs are encouraged to specify in the guide specific items or elements of unclassified information
3803 or CUI to be protected. Cite (U) or the appropriate CUI designation (see DoDI 5200.48 for further
3804 information on CUI designations).

3805
3806
3807 4. DATA COMPILATION CONSIDERATIONS. Posting of unclassified defense and U.S.
3808 Government information to publicly accessible internet sites makes access to the information from
3809 anywhere in the world easy and affordable. Search capabilities and data mining tools make
3810 discovery and correlation of available information fast and simple. This ability to discover and
3811 analyze militarily-relevant data creates the need to pay particular attention to classified
3812 compilations of data elements. Where specific combinations of unclassified data elements are
3813 known to be classified, CONSISTENTLY withholding specified data elements from public Internet
3814 posting and, to the extent possible consistent with statute and other regulations, public release can
3815 mitigate the ability of others to create the classified compilation. Thus, OCAs should consider
3816 including in SCGs, where appropriate, prohibitions on posting one or more of the specific data
3817 elements that are known to make up a classified compilation of unclassified data elements to

3818 publicly accessible internet sites. See section 15 of Enclosure 4 for guidance on classification by
3819 compilation.

3820
3821
3822 5. APPROVAL OF SCGs. An OCA shall personally approve, in writing, the SCG. This OCA
3823 shall be an official who:

3824
3825 a. Has program or supervisory responsibility for the information, or is the senior agency
3826 official for DoD or for the originating Military Department.

3827
3828 b. Is authorized to originally classify information at the highest level the SCG specifies.

3829
3830
3831 6. DISTRIBUTION OF SCGs. The originating organization shall:

3832
3833 a. Distribute SCGs, signed by the appropriate OCA, to those organizations and activities that
3834 may classify information the guide covers. SCGs may not be included or transmitted by means of
3835 an official DoD issuance (e.g., Instruction or Manual).

3836
3837 b. Forward one copy of each SCG to the Defense Office of Prepublication and Security
3838 Review, Washington Headquarters Service. SCGs that cover SCI or SAP information and that
3839 contain information that requires special access controls are exempt from this requirement. The
3840 mailing address to use is:

3841
3842 Department of Defense
3843 Defense Office of Prepublication and Security Review 1155 Defense Pentagon
3844 Washington, DC 20301-1155

3845
3846 c. Provide one copy of each approved guide, signed by an OCA, but not those covering top
3847 secret, SCI, or SAP information, or guides deemed by the guide's approval authority to be too
3848 sensitive for automatic secondary distribution) to the Administrator, DTIC, along with DD Form
3849 2024. DTIC will not accept the DD Form 2024 if it is not completely filled out and not signed by
3850 the appropriate agency. Each guide furnished to DTIC shall bear the appropriate distribution
3851 statement required by Reference (am) (see also Enclosure 3 of Volume 2 for guidance on
3852 distribution statements). DTIC's mailing address is:

3853
3854 Defense Technical Information Center
3855 ATTN: DTIC-OA (Security Classification Guides) 8725 John J. Kingman Road
3856 Fort Belvoir, VA 22060-6218
3857 For information on electronic submissions, contact TR@dtic.mil.

3858
3859 d. Provide one copy of each approved guide to the activity security manager.

3860
3861 e. Provide one copy to the DoD Component declassification program manager.

3862
3863 **f. *(Added)(DAF) All DAF SCGs must be processed through the OCA's servicing IP**
3864 **office. (T-1).**

3865
3866 **(1) *(Added)(DAF) The IP office will review the SCG and make certain the guide has**

...

3867 clear and precise classification guidance, proper declassification instructions, is formatted
 3868 correctly, and marked properly. (T-1). A copy of the final SCG must be forwarded to the
 3869 servicing MAJCOM/FLDCOM IP. (T-1).

3870
 3871 (2) *(Added)(DAF) The MAJCOM/FLDCOM IP will send a copy of the final SCG to
 3872 the SAF/AAZ, Information Security Program Manager and AFDO. (T-1).

3873
 3874 g. *(Added)(DAF) The appendix to this enclosure, is the new standard format for all
 3875 DAF SCGs and cannot be supplemented. Ensure SCGs are processed in accordance with
 3876 enclosure 6 of this volume, to include checking DTIC to validate whether or not there is an
 3877 existing SCG, prior to making a new original classification determination.

3878
 3879
 3880 7. INDEX OF SCGs. Classification guidance (e.g., SGCs or memorandums) issued in
 3881 accordance with this enclosure shall be indexed in an on-line accessible database maintained by
 3882 DTIC. Originators of the SCGs shall submit DD Form 2024 to the Administrator, DTIC, upon
 3883 approval of the guide, with each update, revision, or review, or whenever the guide is cancelled or
 3884 superseded. If the originator determines that listing the SCG in the DTIC-maintained database is
 3885 inadvisable for security reasons (e.g., involves SAPs), the originator shall separately report issuing
 3886 the guide to the Director of Security, USD(I&S), and explain why the guide should not be listed.

3887
 3888
 3889 8. REVIEW OF SCGs. Each SCG shall be reviewed by the issuing OCA at least once every five
 3890 (5) years to ensure it is current and accurate. When necessitated by significant changes in a E.O. or
 3891 by changes in operations, plans, or programs, reviews will be conducted sooner. The OCA shall
 3892 make changes identified as necessary in the review process. If no changes are required, the OCA
 3893 shall submit to DTIC a new DD Form 2024 with the date of the next required review and annotate
 3894 the record copy of the guide with this fact and the date of the review. DTIC will send reminders to
 3895 organizations as security classification guides near their 5-year required reviews.

3896
 3897
 3898 9. REVISION OF SCGs. SCGs shall be revised whenever necessary to promote effective
 3899 derivative classification. Revised SCGs shall be reported as required in section 7 of this enclosure.

3900
 3901
 3902 10. CANCELLING SCGs

3903
 3904 a. SCGs shall be canceled only when:

3905
 3906 (1) All information the guide specified as classified has been declassified; or

3907
 3908 (2) A new SCG incorporates the classified information covered by the old guide and there
 3909 is no reasonable likelihood that any information not incorporated by the new guide shall be the
 3910 subject of derivative classification. The impact on systems, plans, programs, or projects must be
 3911 considered when deciding to cancel a SCG.

3912
 3913 b. Upon canceling a SCG, the responsible official shall consider the need for publishing a
 3914 declassification guide, according to section 4 of Enclosure 5.

3915

3916 c. The OCA, or successor organization, shall maintain a record copy of any canceled SCG, as
3917 required by Reference (aw).

3918
3919
3920 11. REPORTING CHANGES TO SCGs. Revision, reissuance, review, supersession, and
3921 cancellation of a guide shall be reported to DTIC using DD Form 2024, according to section 7 of
3922 this enclosure. Copies of changes, reissued guides, and cancellation notices will be distributed
3923 according to section 6 of this enclosure.

3924
3925
3926 12. FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEWS. As periodically directed by
3927 the USD(I&S), but at least every five (5) years, the DoD Component Heads shall accomplish a
3928 comprehensive review of all classification guidance issued by the DoD Component.

3929
3930 a. Reviews shall ensure the DoD Component's classification guidance reflects current
3931 conditions. The reviews shall also identify classified information that no longer requires protection
3932 and can be declassified.

3933
3934 b. Reviews shall focus on a review of SCGs, but should consider all forms of classification
3935 guidance issued (e.g., memorandums).

3936
3937 c. Reviews shall include an evaluation of classified information to determine if it continues to
3938 meet the standards for classification specified in section 1 of Enclosure 4 of this Volume, using a
3939 current assessment of likely damage.

3940
3941 d. OCAs, DoD Component subject matter experts, and users of the classification guidance
3942 shall be consulted to provide a broad range of perspectives. Contributions of subject matter experts
3943 with sufficient expertise in narrow specializations must be balanced by the participation of
3944 managers and planners who have broader organizational vision and relationships. Additionally, to
3945 the extent practicable, input should also be obtained from external subject matter experts and
3946 external users of the classification guidance.

3947
3948 e. Detailed reports summarizing results and findings shall be prepared and submitted in
3949 accordance with the direction provided and shall be unclassified and releasable to the public, except
3950 when the existence of the guide or program is itself classified. USD(I&S) shall provide a
3951 composite DoD report to ISOO and release an unclassified version to the public.

3952
3953 **f. (Added)(DAF) SAF/AA will coordinate the fundamental classification guidance review**
3954 **and provide a detailed summary to USD(I&S).**
3955

(Added)(DAF) APPENDIX TO ENCLOSURE 6*SECURITY CLASSIFICATION GUIDE TEMPLATE**

All classification markings and declassification guidance are for instructional purposes only

1. ***(Added)(DAF) The table format cannot be changed without prior approval from the SAF/AAZ, Information Security Program Manager. The two exceptions are:**

a. **(Added)(DAF) Non-acquisition SCGs that cover specific activity operations/capabilities; or, tactics, techniques and procedures.**

b. **(Added)(DAF) If a section is “not applicable,” delete it.**

2. ***(Added)(DAF) To ensure proper safeguarding, SCGs will be marked CUI, under the “OPSEC” category (at minimum).**

3. ***(Added)(DAF) Delete the examples in each table prior to use. On the cover page, signature page, and sections 1 and 2, only complete the areas with the [bracketed] font. More descriptive details of what should be covered in sections 2 – 8 can be found in DoDM 5200.45, *Instructions for Developing Security Classification Guides*.**

- **COVER PAGE**
- **SIGNATURE PAGE**
- **SECTION 1 – GENERAL INSTRUCTIONS**
- **SECTION 2 – OVERALL EFFORT**
- **SECTION 3 – ADMINISTRATIVE DATA**
- **SECTION 4 – PERFORMANCE AND CAPABILITIES**
- **SECTION 5 – SPECIFICATIONS**
- **SECTION 6 – VULNERABILITIES AND WEAKNESSES**
- **SECTION 7 – HARDWARE**
- **SECTION 8 – CRITICAL ELEMENTS (OPTIONAL)**

INTENTIONALLY LEFT BLANK

[CUI or CLASSIFICATION¹]

[INSERT NAME OF THE SYSTEM, PLAN, PROGRAM, OR PROJECT]
SECURITY CLASSIFICATION GUIDE



OFFICE OF PRIMARY RESPONSIBILITY: See SECTION 1, paragraph 3.

ISSUANCE DATE: [YYYYMMDD] or [DD MONTH YYYY] (if this is a revision, this is the date the SCG was originally created)

REVISION DATE: [YYYYMMDD] or [DD MONTH YYYY] (delete if not applicable)

[DISTRIBUTION STATEMENT B, C, D, E]: If Distribution Statement F is utilized, the OCA must comply with guidance in DoDI 5230.24, *Distribution Statements on Technical Documents*. (Note: only utilize a distribution statement if the CUI category is “controlled technical information” or “export-controlled”).

EXPORT CONTROL WARNING (see DoDI 5230.24 for verbiage; delete if not applicable)

Controlled by: [Name of Office] CUI Category: OPSEC (at minimum) Dissemination Control: See Table 2, of DoDI 5200.48 POC: [phone and email address]
--

[CUI or CLASSIFICATION¹]

¹Place in the header and footer of each page

[CUI or CLASSIFICATION]

SIGNATURE PAGE

**[INSERT NAME OF THE SYSTEM, PLAN, PROGRAM, OR PROJECT]
SECURITY CLASSIFICATION GUIDE**

PREPARED BY:

[Name, title (Rank)]

Signature

APPROVED BY:

[OCA Name, title (Rank)]

Signature

[CUI or CLASSIFICATION]

[CUI or CLASSIFICATION]

SECTION 1 – GENERAL INSTRUCTIONS

1. PURPOSE. To provide instructions and guidance on the classification of information involved in [**name of the system, plan, program, project, or mission**], using an unclassified identification of the effort.

2. AUTHORITY. This guide is issued under the authority of Executive Order (E.O.) 13526 and DoDM5200.01V1_AFMAN16-1404V1. This guide constitutes authority and may be cited as the basis for classification, regrading, or declassification of information and material involved in [**identify the effort**]. Changes in classification required by application of this guide shall be made immediately. Information identified in this guide for protection as classified information is classified by [**complete title or position of the OCA**].

3. OFFICE OF PRIMARY RESPONSIBILITY (OPR). This guide is issued by, and all inquiries concerning content and interpretation as well as any recommendations for changes, should be addressed to:

- [**Office Name**]
- [**Office Symbol (or code)**]
- [**Mailing address (or email)**]
- [**Phone**]
- [**MAJCOM/FLDCOM**]

4. CLASSIFICATION RECOMMENDATIONS AND CHALLENGES. If at any time, any of the security classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this guide until such time as a final decision is made on the challenge by appropriate authority. All classification recommendations and challenges should be addressed to the OPR (above).

5. REPRODUCTION, EXTRACTION AND DISSEMINATION. Authorized recipients of this guide may reproduce, extract, and disseminate the contents of this guide, as necessary, for application by specified groups involved in [**identify the effort**], including industrial activities. Copies of separate guides issued to operating activities in application of this guide shall be sent to the OPR.

6. PUBLIC RELEASE. The fact that this guide shows certain details of information to be unclassified, or controlled unclassified information, does not allow for automatic public release of this information. DoD information requested by the media, or members of the public, or proposed for release to the public by DoD personnel, or their contractors, shall be processed in accordance with AFI 35-101, *Public Affairs Operations*. Proposed public disclosures regarding [**identify the effort**] shall be processed through the OPR in paragraph 3 above.

[CUI or CLASSIFICATION]

[CUI or CLASSIFICATION]

7. FOREIGN DISCLOSURE. Any disclosure to foreign officials of information classified by this guide shall be in accordance with the procedures set forth in DoD Directive 5230.11. If a country with which the DoD has entered into a reciprocal procurement memorandum of understanding or offset arrangement, expresses an interest in this effort, a foreign disclosure review should be conducted prior to issuance of a solicitation.

8. CONTROLLED UNCLASSIFIED INFORMATION (CUI)

a. Guidance for the proper usage, marking, handling, and dissemination of CUI is covered in DoDI 5200.48. FOR OFFICIAL USE ONLY (FOUO) is no longer authorized.

b. The CUI Designation Indicator (see below) must be included on the first page or cover of all documents containing CUI, including documents comingled with classified information.

Controlled by: [Name of DoD Component] (only if not in letterhead)
 Controlled by: [Name of Office]
 CUI Category: [List category(ies) of CUI]
 Distribution/Dissemination Control:
 POC: [Phone or email address]

9. CLASSIFICATION AUTHORITY BLOCK. The classification authority block must appear on the face of the document. While placement on the bottom left of the page is most typical, whether it is placed on the right or left side or appears as one line is determined by available space.

Classified by: [List name and position title of derivative classifier]
 Derived from: [Concisely cite the source document or SCG]
 Declassify on: [10 years*, 25 years* or Specific Date/Event]

10. DECLASSIFICATION INSTRUCTIONS

a. *10 years from date of original classification – denotes classification would begin from the date of document creation, not from the date of the SCG used to authorize classification.

b. *25 years from date of original classification – denotes classification would begin from the date of document creation, not from the date of the SCG used to authorize classification.

11. ACRONYMS/ DEFINITIONS *[Only include acronyms for which there may be various meanings, to ensure common understanding of the details of information]*

TERM	ACRONYM	DEFINITION

[CUI or CLASSIFICATION]

[CUI or CLASSIFICATION]**SECTION 2 – OVERALL EFFORT**

1. IDENTIFICATION. [Include in this paragraph any necessary statements explaining the classifications, if any, to be assigned to various statements identifying the effort. These statements should be consistent with other program documentation.]

2. GOAL, MISSION, PURPOSE. [Include in this paragraph any necessary statements identifying information concerning the purpose of the effort that can be released as unclassified and that which must be classified. Take care to ensure that unclassified statements do not reveal classified information.]

3. END ITEM. [Include in this paragraph statements of the classification to be assigned to the end products of the effort, whether paperwork or hardware. In this connection it is important to distinguish between classification required to protect the fact of the existence of a completed end item, and classification required because of what the end item contains or reveals. In some instances classified information pertaining to performance, manufacture, or composition of incorporated parts or materials is not ascertainable from mere use of or access to the end item. In others, the classifiable information is that which concerns total performance, capabilities, vulnerabilities, or weaknesses of the end item itself, rather than any of the parts or materials.]

INTENTIONALLY LEFT BLANK

[CUI or CLASSIFICATION]

[CUI or CLASSIFICATION]

SECTION 3 – ADMINISTRATIVE DATA

TOPIC, DESCRIPTION, or INFORMATION REVEALING	CLASS	REASON/ DATE OF ORIGINAL DECISION	DECLASSIFY ON (date or event)	UNCLASSIFIED DESIGNATION	REMARKS
1. Delivery dates of critical components	Confidential	1.4(a) 20110505	Upon delivery		
2. Out-year milestones				CUI See Remarks	CUI Category: OPSEC Dissemination Control: FEDCON
3. Budget data				CUI See Remarks	Category: BUDG Dissemination Control: FED ONLY Unclassified upon release to Congress
4. Organizational Charts				Unclassified	

[CUI or CLASSIFICATION]

[CUI or CLASSIFICATION]

SECTION 4 – PERFORMANCE AND CAPABILITIES

TOPIC, DESCRIPTION, or INFORMATION REVEALING	CLASS	REASON/ DATE OF ORIGINAL DECISION	DECLASSIFY ON <i>(date or event)</i>	UNCLASSIFIED DESIGNATION	REMARKS
<i>1. Range:</i>					
<i>a. Effective range of ABC missile (Actual)</i>	<i>Secret</i>	<i>1.4(a) 20110505</i>	<i>25 Years* See Remarks</i>		<i>*See section 1, paragraph 10 (applies throughout)</i>
<i>b. Effective range of ABC missile (Predicted)</i>				<i>Unclassified</i>	
<i>2. Commercial receiver (Model No. XXX)</i>	<i>See Remarks</i>	<i>See Remarks</i>	<i>See Remarks</i>		<i>Classification guidance for this topic is covered under XXX Commercial Receiver SCG dated YYYYMMDD (or subsequent revisions)</i>

[CUI or CLASSIFICATION]

[CUI or CLASSIFICATION]

SECTION 7 – HARDWARE

TOPIC, DESCRIPTION, or INFORMATION REVEALING	CLASS	REASON/ DATE OF ORIGINAL DECISION	DECLASSIFY ON (date or event)	UNCLASSIFIED DESIGNATION	REMARKS
<i>I. AN/APR-XXXX:</i>					
<i>a. Internal view</i>	<i>Confidential See Remarks</i>	<i>1.4(a) 20110505</i>	<i>10 Years</i>		<i>Image is unclassified if the flux capacitor is not visible</i>
<i>b. External view</i>				<i>Unclassified</i>	
<i>c. Preamplifier</i>				<i>CUI See Remarks</i>	<i>CUI Category: CTI Distribution Statement E</i>
<i>d. Analyzer Unit:</i>					
<i>(1) Displays and controls powered on</i>	<i>Secret</i>	<i>1.4(a) 20110505</i>	<i>Once powered down</i>		
<i>(2) Powered down</i>				<i>Unclassified</i>	

[CUI or CLASSIFICATION]

GLOSSARYPART I. ABBREVIATIONS AND ACRONYMS

ACCM	Alternative Compensatory Control Measures
AO	Authorizing Official
B&P	Bid and Proposal
CI	Counterintelligence
CNWDI	Critical Nuclear Weapon Design Information
COMSEC	Communication Security
CUI	Controlled Unclassified Information
CUIO	Controlled Unclassified Information Office
CUSR	Central United States Registry
DASD(NM)	Deputy Assistant Secretary of Defense for Nuclear Matters
DCSA	Defense Counterintelligence and Security Agency
DD	DoD
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoDD	DoD Directive
DoD CIO	DoD Chief Information Officer
DoDI	DoD Instruction
DoDM	DoD Manual
DOE	Department of Energy
DTIC	Defense Technical Information Center
DUSD(I&S)	Deputy Under Secretary of Defense for Intelligence & Security
E.O.	Executive Order
FFRDC	Federally Funded Research and Development Center
FGI	Foreign Government Information
FRD	Formerly Restricted Data
GIG	Global Information Grid
GS	General Schedule
IR&D	Independent Research and Development
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
ISSM	Information System Security Officer
IT	Information Technology
JPAS	Joint Personnel Adjudication System
JWICS	Joint Worldwide Intelligence Communications System
MDR	Mandatory Declassification Review
MR	Manual Review
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NC2-ESI	Nuclear Command & Control-Extremely Sensitive Information
NDC	National Declassification Center
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSC	National Security Council
OADR	Originating Agency's Determination Required
OCA	Original Classification Authority

OPM	Office of Personnel Management
OPR	Office of Primary Responsibility
OPSEC	Operations Security
PA	Public Affairs
RD	Restricted Data
SAO	Senior Agency Official
SAP	Special Access Program
SAPCO	Special Access Program Central Office
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SETA	Security, Education, Training and Awareness
SF	Standard Form
SIPRNET	Secret Internet Protocol Router Network
SSO	Special Security Officer
TSCA	Top Secret Control Assistant
TSCO	Top Secret Control Officer
UCMJ	Uniform Code of Military Justice
USC	United States Code
USD(I&S)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USSAN	United States Security Authority for NATO
WHS	Washington Headquarters Services

6
7
8
9

***(Added)(DAF) PART IA. ACRONYMS**

AA	Administrative Assistant
AFDO	Air Force Declassification Office
AFOTEC	Air Force Operational Test and Evaluation Center
ANG	Air National Guard
CC	commander
CD	deputy commander
CV	vice commander
DAF	Department of the Air Force
DAFI	Department of the Air Force Instruction
DAFMAN	Department of the Air Force Manual
DRU	Direct Reporting Unit
FLDCOM	Field Command
FOA	Field Operating Agency
HAF	Headquarters Air Force
HAFMD	Headquarters Air Force Mission Directive
IDA	initial denial authority
IG	Inspector General
IGEMS	Inspector General Evaluation Management System
IP	information protection
MAJCOM	Major Command
MD	mandatory declassification
MICT	Management Internal Control Toolset
PED	portable electronic devices
SAF	Secretary Air Force

...

SAC	self-assessment checklist
SecAF	Secretary of the Air Force
SPE	Security Program Executive
STIP	Scientific and Technical Information Program
TFNI	Transclassified Foreign Nuclear Information
UCNI	Unclassified Controlled Nuclear Information
USSF	United States Space Force

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47

...

48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Volume.

Access. The ability or opportunity to obtain knowledge of classified information.

Accessioned records. Records of permanent historical value in the legal custody of NARA.

Activity Security Manager

The individual specifically designated in writing and responsible for the activity's information security program, which ensures that classified information (except SCI which is the responsibility of the SSO appointed by the senior intelligence official) and CUI are properly handled during their entire life cycle. This includes ensuring information is appropriately identified, marked, stored, disseminated, disposed of, and accounted for, as well as providing guidance on the handling of security incidents to minimize adverse effects and ensure that appropriate corrective action is taken. The security manager may be assigned responsibilities in other security disciplines such as personnel and physical security, etc. The activity security manager implements the information security program guidance established by this Manual and the Component senior agency official.

(Added)(DAF) An example of an activity security manager is the installation Chief, IP or any members of their staff. This term may also be associated with an organization where the commander/director decides they have the need for fulltime security specialist; or opts out of host installation Information Protection support, as administered in accordance with a Support Agreement.

Agency. Any Executive agency as defined in section 105 of Reference (ay); any Military Department as defined in section 102 of Reference (bd); and any other entity within the Executive Branch that comes into the possession of classified information.

(Added)(DAF) Assistant security manager. A U.S. government civilian or military member designated, in writing, to assist with the implementation, maintenance and oversight of information security program. An example of an assistant security manager is a full-time, appointed security specialist managing an information protection program for a commander/director. This role is under the oversight of an activity security manager, at the host installation or a program office at another installation.

Authorized person. A person who has a favorable determination of eligibility for access to classified information, has signed an SF 312 nondisclosure agreement, and has a need to know for the specific classified information in the performance of official duties.

Automatic declassification. The declassification of information based solely 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 established pursuant to Reference (d).

Classification. The act or process by which information is determined to be classified information.

...

99

100 Classification guidance. Any instruction or source that prescribes the classification of specific
101 information.

102

103 Classified National Security Information. Information that has been determined pursuant to
104 Reference (d), or any predecessor order, to require protection against unauthorized disclosure and is
105 marked to indicate its classified status when in documentary form.

106

107 Classifier. An individual who makes a classification determination and applies a security
108 classification to information or material. A classifier may be an OCA or a person who derivatively
109 assigns a security classification based on a properly classified source or a classification guide.

110

111 Collateral information. All national security information classified confidential, secret, or top secret
112 under the provision of an E.O. for which special systems of compartmentation (such as SCI or SAP)
113 are not formally required.

114

115 Compilation. An aggregation of preexisting items of information.

116

117 Compromise. An unauthorized disclosure of classified information.

118

119 COMSEC. The protection resulting from all measures designed to deny unauthorized persons
120 information of value that might be derived from the possession and study of telecommunications and
121 to ensure the authenticity of such communications. COMSEC includes crypto-security, TEMPEST,
122 transmission security, and physical security of COMSEC material and information.

123

124 Confidential source. Any individual or organization that has provided, or that may reasonably be
125 expected to provide, information to the United States on matters pertaining to the national security
126 with the expectation that the information or relationship, or both, are to be held in confidence.

127

128 Control. The authority of the agency that originates information, or its successor in function, to
129 regulate access to the information.

130

131 CUI. Unclassified information requiring safeguarding or dissemination controls, pursuant to and
132 consistent with applicable law, regulations, and Government-wide policies. Some CUI may also be
133 export-controlled or protected by contract. Release or disclosure of CUI to foreign governments or
134 international organizations must be in accordance with Reference (z) and other policy and procedures
135 established by the USD(P) (See DoDI 5200.48 for further information regarding CUI).

136

137 Date of original classification. The date a document is determined to be classified. For example,
138 classification would begin from the date a document is created, not from the date of any security
139 classification guide used to authorize classification of that document.

140

141 Damage to the national security. Harm to the national defense or foreign relations of the United
142 States from the unauthorized disclosure of information, taking into consideration such aspects of the
143 information as the sensitivity, value, utility, and provenance of that information.

144

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

147

148 Declassification authority

149

...

150 The official who authorized the original classification, if that official is still serving in the same
151 position;

152
153 The originator's current successor in function, if that individual has OCA;

154
155 A supervisory official of either the originator or his or her successor in function, if the
156 supervisory official has OCA; or

157
158 Officials delegated declassification authority in writing by the agency head or the SAO.

159
160 Declassification guide. Written instructions issued by a declassification authority that describes the
161 elements of information regarding a specific subject that may be declassified and the elements that
162 must remain classified. May also be a guide providing classification and declassification instructions
163 specifically for information that is 25 years old or older and of permanent historical value. A
164 declassification guide is the most commonly used vehicle for obtaining ISCAP approval of 25-year
165 exemptions from the automatic declassification provisions of Reference (d).

166
167 Defense Intelligence Components. All DoD organizations that perform national intelligence, Defense
168 Intelligence, and intelligence-related functions, including: the Defense Intelligence Agency; the
169 National Geospatial-Intelligence Agency, the National Reconnaissance Office, the National Security
170 Agency/Central Security Service, and the intelligence elements of the Active and Reserve
171 components of the Military Departments, including the United States Coast Guard when operating as
172 a service in the Navy.

173
174 Derivative classification. Incorporating, paraphrasing, restating, or generating in new form
175 information that is already classified, and marking the newly developed material consistent with the
176 classification markings that apply to the source information. Includes the classification of information
177 based on classification guidance. The duplication or reproduction of existing classified information is
178 not derivative classification.

179
180 Distribution statement. A statement used on a technical document to denote the extent of its
181 availability for secondary distribution, release, and disclosure without additional approvals or
182 authorizations. A distribution statement is distinct from and in addition to a security classification
183 marking and any dissemination control markings included in the banner line. A distribution statement
184 is also required on security classification guides submitted to DTIC.

185
186 Document. Any recorded information, regardless of the nature of the medium or the method or
187 circumstances of recording. This includes any physical medium in or on which information is
188 recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic
189 storage media.

190
191 Downgrading. A determination by a declassification authority that information classified and
192 safeguarded at a specified level shall be classified and safeguarded at a lower level.

193
194 Element of the Intelligence Community. See Intelligence Community.

195
196 Equity. For purposes of classification management, information originally classified by or under the
197 control of an agency.

198
199 Exception. An approved permanent exclusion or deviation from an information security standard or
200 requirement, as specified in this Volume.

...

201
202 Exempted. Nomenclature and marking indicating information has been determined to fall within an
203 enumerated exemption from automatic declassification in accordance with Reference (d).

204
205 FGI

206
207 Information provided to the U.S. Government by a foreign government or governments, an
208 international organization of governments, or any element thereof, with the expectation that the
209 information, the source of the information, or both, are to be held in confidence;

210
211 Information produced by the U.S. Government pursuant to or as a result of a joint
212 arrangement with a foreign government or governments, or an international organization of
213 governments, or any element thereof, requiring that the information, the arrangement, or both, are to
214 be held in confidence; or

215
216 Information received and treated as FGI pursuant to the terms of a predecessor order to
217 Reference (d).

218
219 File series. File units or documents arranged according to a filing system or kept together because
220 they relate to a particular subject or function, result from the same activity, document a specific kind
221 of transaction, take a particular form, or have some other relationship arising out of their creation,
222 receipt, or use, such as restrictions on access or use. Also documentary material, regardless of its
223 physical form or characteristics, that is arranged in accordance with a filing system or maintained as a
224 unit because it pertains to the same subject, function, or activity.

225
226 File series exemption. An exception to the 25-year automatic declassification provisions of
227 Reference (d). This exception applies to entire blocks of records (i.e., “file series,” within an
228 agency’s records management program). To qualify for this exemption, the file series must be replete
229 with exemptible information.

230
231 FRD. Information removed from the RD category upon a joint determination by the Department of
232 Energy (or antecedent agencies) and the Department of Defense that such information relates
233 primarily to the military utilization of atomic weapons and that such information can be safeguarded
234 adequately as classified defense information. For purposes of foreign dissemination, this information
235 is treated in the same manner as RD.

236
237 Heads of DoD activities. Heads, either military or civilian, of organizations, commands, and staff
238 elements subordinate to a DoD Component, with jurisdiction over and responsibility for the execution
239 of the organization’s mission and functions, including its information security program. The official
240 may carry the title of commander, commanding officer, or director, or other equivalent title.

241
242 Human intelligence source. People who provide intelligence directly; individuals associated with
243 organizations (such as foreign government entities and intelligence services) who willingly share
244 intelligence information with the U.S.; individuals and organizations who facilitate the placement or
245 service of technical collection means that could not succeed without their support; and foreign
246 citizens who are identified as of an intelligence interest to the U.S. with a reasonable expectation that
247 they will provide information or services in the future. Information that may reveal the identities of
248 people upon whom the U.S. relies for information, access to information, or cooperation leading to
249 obtaining information is considered to potentially reveal human intelligence sources.

250
251 Information. Any knowledge that can be communicated or documentary material, regardless of its

...

252 physical form, or characteristics, that is owned by, produced by or for, or is under the control of the
253 U.S. Government.

254

255 Information security. The system of policies, procedures, and requirements established in accordance
256 with Reference (d) to protect information that, if subjected to unauthorized disclosure, could
257 reasonably be expected to cause damage to national security. The term also applies to policies,
258 procedures, and requirements established to protect unclassified information that may be withheld
259 from release to the public pursuant to E.O., statute, or regulation.

260

261 **(Added)(DAF) Inspector General Evaluation Management System (IGEMS). IGEMS (to**
262 **include the classified version) facilitates scheduling, planning, inspecting, and report writing for**
263 **IG inspections. IGEMS is also used to assign, monitor, and close (if applicable) all findings**
264 **(strengths, recommended improvement areas, deficiencies) identified during the inspection**
265 **process. The system is comprised of an open architecture which facilitates manual enterprise-**
266 **level trending analysis and cross communication with normalized data and standardized**
267 **reporting.**

268

269 Integral file block. A distinct component of a file series that should be maintained as a separate unit
270 to ensure the integrity of the records. An integral file block may consist of a set of records covering
271 either a specific topic or a range of time, such as a Presidential administration or a five (5) year
272 retirement schedule within a specific file series that is retired from active use as a group. For
273 purposes of automatic declassification, integral file blocks shall contain only records dated within ten
274 (10) years of the oldest record in the file block.

275

276 Integrity. The state that exists when information is unchanged from its source and has not been
277 accidentally or intentionally modified, altered, or destroyed.

278

279 Intelligence Community. An element or agency of the U.S. Government identified in or designated
280 pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of
281 Reference (ah).

282

283 International program. Any program, project, contract, operation, exercise, training, experiment, or
284 other initiative that involves a DoD Component or a DoD contractor and a foreign government,
285 international organization, or corporation that is located and incorporated to do business in a foreign
286 country.

287

288 ***(Added)(DAF) Management Internal Control Toolset. MICT is a DAF program of record and**
289 **provides units a tool for managing their self-assessment programs. It also provides a means to**
290 **communicate a unit's program health using SACs and HAF SAC fragmentary orders. MICT**
291 **also provides supervisors and the command chain (from squadron commander to SecAF) tiered**
292 **visibility into user-selected compliance reports and program status as well as indications of**
293 **program health across functional and command channels. MICT also helps facilitate the HAF**
294 **SAC fragmentary order programs by gathering time-sensitive data in an expeditious manner.**

295

296 Material. Any product or substance on or in which information is embodied.

297

298 National Security. The national defense or foreign relations of the U.S. National Security includes
299 defense against transnational terrorism.

300

301 National security system. Defined in section 3542(b)(2) of Reference (av).

302

...

303 Need-to-know. A determination that a prospective recipient requires access to specific classified
304 information in order to perform or assist in a lawful and authorized governmental function.

305
306 Network. A system of two or more computers that can exchange data or information.

307
308 Newly discovered records. Records that were inadvertently not reviewed prior to the effective date of
309 automatic declassification because the Agency declassification authority was unaware of their
310 existence.

311
312 OCA. An individual authorized in writing, either by the President, the Vice President, or by agency
313 heads or other officials designated by the President, to originally classify information (i.e., to classify
314 information in the first instance).

315
316 Original classification. An initial determination that information requires, in the interests of national
317 security, protection against unauthorized disclosure.

318
319 Pass/fail. A declassification technique that regards information at the full document level. Any
320 exemptible portion of a document may result in exemption (failure) of the entire document.
321 Documents that contain no exemptible information are passed and therefore declassified. Documents
322 that contain exemptible information are failed and therefore exempt from automatic declassification.

323
324 Permanent records. Any Federal record that has been determined by NARA to have sufficient value
325 to warrant its preservation in the National Archives of the U.S. Permanent records include all records
326 accessioned by NARA into the National Archives of the U.S. and later increments of the same
327 records, and those for which the disposition is permanent on SF 115, "Request for Records
328 Disposition Authority," approved by NARA on or after May 14, 1973.

329
330 Permanently valuable records. See "records having permanent historical value."

331
332 RD. All data concerning design, manufacture, or utilization of atomic weapons; the production of
333 special nuclear material; or the use of special nuclear material in the production of energy, but not
334 data declassified or removed from the RD category pursuant to section 2162 of The Atomic Energy
335 Act of 1954, as amended.

336
337 Records. The records of an agency and Presidential papers or Presidential records, as those terms are
338 defined in Reference (av), including those created or maintained by a U.S. Government contractor,
339 licensee, certificate holder, or grantee that are subject to the sponsoring agency's control in
340 accordance with the terms of the contract, license, certificate, or grant.

341
342 Records having permanent historical value. Records that the Archivist of the United States has
343 determined should be maintained permanently in accordance with Reference (av).

344
345 Records management. The planning, controlling, directing, organizing, training, promoting, and
346 other managerial activities involved with respect to records creation, records maintenance and use,
347 and records disposition in order to achieve adequate and proper documentation of the policies and
348 transactions of the Federal Government and effective and economical management of agency
349 operations. Within the Department of Defense, records management is implemented by Reference
350 (aw).

351
352 Redaction. For purposes of declassification, the removal of exempted information from copies of a
353 document.

...

354
355 Released to the public. Made available to the general public through any publicly accessible media
356 or method.

357
358 Risk management. The process of identifying, assessing, and controlling risks and making decisions
359 that balance risk with cost and benefits.

360
361 Safeguarding. Measures and controls that are prescribed to protect classified information.

362
363 SAP. A program established for a specific class of classified information that imposes safeguarding
364 and access requirements that exceed those normally required for information at the same
365 classification level. In the DoD, any DoD program or activity (as authorized in Reference (d)),
366 employing enhanced security measures (e.g., safeguarding, access requirements), exceeding those
367 normally required for collateral information at the same level of classification, shall be established,
368 approved, and managed as a DoD SAP in accordance with Reference (q).

369
370 Scheduled records. All records that fall under a NARA-approved records control schedule.

371
372 SCI. Classified information concerning or derived from intelligence sources, methods, or analytical
373 processes that is required to be handled within formal access control systems established by the
374 Director of National Intelligence.

375
376 **(Added)(DAF) Security assistant. Security assistants are U.S. government civilian or military**
377 **personnel who perform administrative security functions, under the direction of their**
378 **commander/director and oversight of an activity security manager. An example of a security**
379 **assistant is an individual with the commander's support staff, who is trained in accordance**
380 **with the scope and complexity of the organization's mission, to generate periodic**
381 **reinvestigation reports and document access in the Defense Information Security System (or**
382 **equivalent), and record non-disclosure agreement completion.**

383
384 Security classification guide. A documentary form of classification guidance issued by an OCA that
385 identifies the elements of information regarding a specific subject that must be classified and
386 establishes the level and duration of classification for each such element.

387
388 Security clearance eligibility. A determination that a person is eligible, in accordance with the
389 standards of Reference (s), for access to classified information.

390
391 ***(Added)(DAF) Self-assessment checklist (SAC). A SAC is a list of available questions which**
392 **allows communication to commanders at each level, within the wing/garrison/delta construct,**
393 **designed to assess compliance based upon commander's intent and direction for the**
394 **organization. In addition, those SACs generated by DAF or MAJCOM/FLDCOM provide**
395 **indicators to the functional community, allowing for a more in-depth understanding of policy**
396 **effects on wing/garrison/delta and below organizations.**

397
398 Self-inspection. The internal review and evaluation of individual DoD Component activities and the
399 DoD Component as a whole with respect to the implementation of the information security program
400 established in accordance with References (b), (d) and (f), and this Manual.

401
402 Senior Agency Official. An official appointed by the head of a DoD Component to be responsible for
403 direction, administration, and oversight of the Component's information security program, to include
404 classification, declassification, safeguarding, and security education and training programs, and for

...

405 the efficient and effective implementation of References (b), (d), (e), and (f) and the guidance in this
 406 Manual. Where used in reference to authorities pursuant to section 5.4(d) of Reference (d), this term
 407 applies only to the senior agency officials of the Military Departments and of the DoD.

408
 409 Senior Intelligence Official. The highest ranking military or civilian charged with direct foreign
 410 intelligence missions, functions, or responsibilities with a department, agency, component, or element
 411 of an Intelligence Community organization. Responsible for direction, administration, and oversight
 412 of the organization's SCI program, to include classification, declassification, safeguarding, and
 413 security education and training programs for the effective implementation of References (b), (j), and
 414 (ad) and the guidance in this Manual.

415
 416 SSO. Individual appointed, in accordance with References (j) and (ad), by the senior intelligence
 417 official to be responsible for the day-to-day security management, operation, implementation, use,
 418 and dissemination of SCI within an activity.

419
 420 Tab. A narrow paper sleeve placed around a document or group of documents in such a way that it is
 421 readily visible.

422
 423 Telecommunications. The preparation, transmission, or communication of information by electronic
 424 means.

425
 426 ***(Added)(DAF) Temporary records. Records approved by the National Archives for disposal
 427 either immediately or after a specified retention period of less than permanent; also called,
 428 disposable records or non-permanent records.**

429
 430 Transferred records. Records transferred to agency storage facilities or a Federal records center.

431
 432 Unauthorized disclosure. Communication or physical transfer of classified or controlled unclassified
 433 information to an unauthorized recipient.

434
 435 Unscheduled records. Records whose final disposition has not been approved by NARA.

436
 437 U.S. entity

438 State, local, or tribal governments

439 State, local, and tribal law enforcement and firefighting entities

440
 441 Public health and medical entities

442
 443 Regional, State, local, and tribal emergency management entities, including State Adjutants

444
 445 General and other appropriate public safety entities

446
 447 Private sector entities serving as part of the Nation's critical infrastructure and/or key resources

448
 449
 450
 451 Violation

452
 453 Any knowing, willful, or negligent action that could reasonably be expected to result in an
 454 unauthorized disclosure of classified information.

455

...

456 Any knowing, willful, or negligent action to classify or continue the classification of information
457 contrary to the requirements of Reference (d), its implementing directives, or this Manual.

458
459 Any knowing, willful, or negligent action to create or continue a special access program contrary
460 to the requirements of Reference (d), Reference (q), or this Manual.

461
462 Waiver. An approved temporary or short-term exclusion or deviation from an information security
463 standard or requirement, as specified in this Volume.

464
465 Weapons of mass destruction. Any weapon of mass destruction as defined in section 1801(p) of
466 Reference (af).