

**BY ORDER OF THE SECRETARY
OF THE AIR FORCE**

**DEPARTMENT OF DEFENSE MANUAL 5200.01,
VOLUME 3**



**DEPARTMENT OF THE AIR FORCE MANUAL
16-1404, VOLUME 3**

12 APRIL 2022

Operations Support

**INFORMATION SECURITY PROGRAM: PROTECTION
OF CLASSIFIED INFORMATION**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no release restrictions on this publication.

OPR: SAF/AAZO

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

Supersedes: DODM 5200.01V3_AFMAN 16-1404V3, 23 December 2020

Pages: 135

This publication implements guidance in Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance* (reference (cr)). The Department of Defense Manual (DoDM) 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*, is printed, word-for-word in regular font, without change. The 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 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 Air Force Instruction (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 Department of the Air Force Instruction (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 appendices 1 and 2 of enclosure 2; appendix 2 of enclosure 3; and appendix 3 of 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 USSF organizations. The term “Wing” includes “Delta,” and “Garrison,” for USSF organizational responsibilities.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Major changes include, updates to compliance checklist, emergency plan oversight requirements, and the implementation of a new security incident tracker. An asterisk (*) indicates newly revised material.



Department of Defense
MANUAL

NUMBER 5200.01, Volume 3

February 24, 2012

Incorporating Change 3, Effective July 28, 2020

USD(I&S)

SUBJECT: DoD Information Security Program: Protection of Classified Information

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 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, E.O. 13556, and part 2001 of title 32, Code of Federal Regulations (CFR) (References (d), (e), and (f)). This combined guidance is known as the DoD Information Security Program.

b. Volume. This Volume:

(1) Provides guidance for safeguarding, storage, destruction, transmission, and transportation of classified information.

(2) Identifies security education and training requirements and processes for handling of security violations and compromise of classified information.

(3) Addresses information technology (IT) issues of which the activity security manager must be aware of.

(4) Incorporates and cancels Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandums (References (g) and (h)).

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. 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 (i)) 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. Employ, maintain and enforce standards for safeguarding, storing, destroying, transmitting, and transporting classified information.

d. Actively promote and implement security education and training throughout the DoD.

e. Mitigate the adverse effects of unauthorized access to classified information by investigating and acting upon reports of security violations and compromises of classified information.

5. RESPONSIBILITIES. See Enclosure 2 of Volume 1.

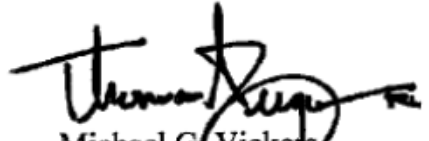
6. PROCEDURES. See Enclosures 2 through 7.

7. INFORMATION COLLECTION REQUIREMENTS. All inspections, investigations, notifications, and audits referred to in this issuance do not require licensing with a Report Control Symbol in accordance with paragraphs 1, 2, 4, and 7 of Volume 1 of DoDM 8910.01 (Reference (j)).

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

9. SUMMARY TO CHANGE 3. The change to this issuance updates references and organizational titles and removes expiration language in accordance with current Chief Management Officer of the DoD direction.

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. Safeguarding
3. Storage and Destruction
4. Transmission and Transportation
5. Security Education and Training
6. Security Incidents Involving Classified Information
7. IT Issues for the Security Manager

Glossary

TABLE OF CONTENTS

1
2
3 ENCLOSURE 1: REFERENCES.....11
4
5 ENCLOSURE 2: SAFEGUARDING.....16
6
7 CONTROL MEASURES.....16
8 PERSONAL RESPONSIBILITY FOR SAFEGUARDING.....16
9 ACCESS TO CLASSIFIED INFORMATION.....16
10 DETERMINING NEED FOR ACCESS.....17
11 EMERGENCY AUTHORITY.....18
12 ACCESS BY INDIVIDUALS OUTSIDE THE EXECUTIVE BRANCH.....20
13 Congress.....20
14 Government Printing Office (GPO).....20
15 Representatives of the Government Accountability Office (GAO).....20
16 Historical Researchers.....20
17 Presidential or Vice Presidential Appointees and Designees.....22
18 Use of Classified Information in Litigation.....22
19 Special Cases.....22
20 VISITS.....22
21 PROTECTION WHEN REMOVED FROM STORAGE.....23
22 END OF DAY SECURITY CHECKS.....23
23 EMERGENCY PLANS.....23
24 USE OF SECURE COMMUNICATIONS.....24
25 REMOVAL OF CLASSIFIED INFORMATION FOR WORK AT HOME.....24
26 Top Secret.....24
27 Secret and Confidential.....24
28 Residential Storage Equipment.....24
29 Classified IT Systems.....25
30 Foreign Country Restriction.....25
31 WORKING PAPERS.....25
32 EQUIPMENT USED FOR PROCESSING CLASSIFIED INFORMATION.....26
33 REPRODUCTION OF CLASSIFIED MATERIAL.....26
34 CLASSIFIED MEETINGS AND CONFERENCES.....27
35 SAFEGUARDING FGI.....30
36 North Atlantic Treaty Organization (NATO) Information.....30
37 Other FGI.....30
38 ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM).....33
39 DoD Proponents for ACCM.....33
40 ACCM Approval.....33
41 Guidance on ACCM Use.....33
42 Prohibited Security Measures.....34
43 Prohibited Uses of ACCM.....34
44 Documentation.....35
45 Annual Reports of ACCM Use.....35
46 Sharing ACCM-Protected Information.....35
47 Contractor Access to ACCM.....35
48 Program Maintenance.....36
49 Safeguarding ACCM Information.....36

50 Security Incidents.....37

51 ACCM Termination.....38

52 Transitioning an ACCM to a SAP.....38

53

54 ***(Added)(DAF) APPENDIX 1 TO ENCLOSURE 2: CLASSIFIED MEETING**

55 **CHECKLIST.....39**

56 ***(Added)(DAF) APPENDIX 2 TO ENCLOSURE 2: EMERGENCY PLAN TEMPLATE...41**

57

58 ENCLOSURE 3: STORAGE AND DESTRUCTION.....43

59

60 GENERAL REQUIREMENTS.....43

61 LOCK SPECIFICATIONS.....43

62 STORAGE OF CLASSIFIED INFORMATION BY LEVEL OF CLASSIFICATION.....44

63 Top Secret.....44

64 Secret.....45

65 Confidential.....45

66 RISK ASSESSMENT.....45

67 CLASSIFIED INFORMATION LOCATED IN FOREIGN COUNTRIES.....46

68 SPECIALIZED STORAGE.....46

69 Military Platforms.....46

70 IT Equipment.....48

71 Map and Plan File Cabinets.....49

72 Modular Vaults.....49

73 Bulky Material.....49

74 PROCURING NEW STORAGE EQUIPMENT.....49

75 SECURITY CONTAINER LABELS.....49

76 EXTERNAL MARKINGS ON CONTAINERS.....50

77 SECURITY CONTAINER INFORMATION.....50

78 COMBINATIONS TO CONTAINERS, VAULTS AND SECURE ROOMS.....51

79 Protecting and Storing Combinations.....51

80 Changing Combinations.....51

81 ENTRANCES TO OPEN STORAGE AREAS FOR CLASSIFIED INFORMATION.....51

82 INSPECTION OF STORAGE CONTAINERS PRIOR TO REMOVAL, REPAIR, ETC.....52

83 NEUTRALIZATION AND REPAIR PROCEDURES.....52

84 STORAGE OF FGI.....52

85 RETENTION OF CLASSIFIED INFORMATION.....52

86 DESTRUCTION OF CLASSIFIED INFORMATION.....53

87 TECHNICAL GUIDANCE ON DESTRUCTION METHODS.....53

88 Crosscut Shredders.....54

89 Pulverizers and Disintegrators.....54

90 Pulping.....54

91 DESTRUCTION PROCEDURES.....54

92

93 APPENDIX 1 TO ENCLOSURE 3: PHYSICAL SECURITY STANDARDS.....56

94 ***(Added)(DAF) APPENDIX 2 TO ENCLOSURE 3: SECURITY CONTAINER, VAULT**

95 **DOOR AND SECURE ROOM VISUAL INSPECTION CHECKLIST.....65**

96

97

98 ENCLOSURE 4: TRANSMISSION AND TRANSPORTATION.....66

99		
100	TRANSMISSION AND TRANSPORTATION PROCEDURES.....	66
101	DISSEMINATION OUTSIDE THE DEPARTMENT OF DEFENSE.....	66
102	TRANSMISSION OF TOP SECRET INFORMATION.....	67
103	TRANSMISSION OF SECRET INFORMATION.....	68
104	TRANSMISSION OF CONFIDENTIAL INFORMATION.....	70
105	TRANSMISSION OF CLASSIFIED INFORMATION AND MATERIAL TO FOREIGN	
106	GOVERNMENTS.....	70
107	SECURITY REQUIREMENTS FOR TRANSFERS OF DEFENSE ARTICLES TO	
108	AUSTRALIA AND THE UNITED KINGDOM WITHOUT AN EXPORT LICENSE OR	
109	OTHER WRITTEN AUTHORIZATION.....	71
110	Background.....	71
111	Applicability.....	71
112	Marking.....	71
113	Transfer.....	73
114	USE OF SECURE COMMUNICATIONS FOR TRANSMISSION OF CLASSIFIED	
115	INFORMATION.....	73
116	Computer-to-Computer Transmission.....	73
117	Facsimile (Fax) Transmission.....	73
118	Telephone.....	74
119	SHIPMENT OF BULK CLASSIFIED MATERIAL AS FREIGHT.....	74
120	PREPARATION OF MATERIAL FOR SHIPMENT.....	74
121	USE OF BRIEFCASES OR ZIPPERED POUCHES FOR HAND-CARRYING CLASSIFIED	
122	MATERIAL.....	75
123	ESCORT, COURIER, OR HAND-CARRY OF CLASSIFIED MATERIAL.....	76
124	Authority.....	76
125	Packaging Requirements.....	76
126	Responsibilities.....	76
127	Customs, Police and Immigration.....	77
128	Disclosure Authorization.....	77
129	ESCORT, COURIER, OR HAND-CARRY AUTHORIZATION.....	77
130	HAND-CARRYING OR ESCORTING CLASSIFIED INFORMATION ON COMMERCIAL	
131	AIRCRAFT.....	78
132		
133	APPENDIX: TRANSFER OF CLASSIFIED INFORMATION OR MATERIAL TO FOREIGN	
134	GOVERNMENTS.....	80
135		
136	ENCLOSURE 5: SECURITY EDUCATION AND TRAINING.....	86
137		
138	REQUIREMENT.....	86
139	SECURITY EDUCATION AND TRAINING RESOURCES.....	86
140	INITIAL ORIENTATION.....	86
141	SPECIAL TRAINING REQUIREMENTS.....	89
142	OCA TRAINING.....	90
143	DECLASSIFICATION AUTHORITY TRAINING.....	93
144	ANNUAL REFRESHER TRAINING.....	93
145	CONTINUING SECURITY EDUCATION AND TRAINING.....	94
146	TERMINATION BRIEFINGS.....	94
147	MANAGEMENT AND OVERSIGHT TRAINING.....	95

148	PROGRAM OVERSIGHT.....	96
149		
150	ENCLOSURE 6: SECURITY INCIDENTS INVOLVING CLASSIFIED INFORMATION.....	97
151		
152	INTRODUCTION.....	97
153	CONSEQUENCES OF COMPROMISE.....	98
154	REPORTING AND NOTIFICATIONS.....	98
155	CLASSIFICATION OF REPORTS.....	100
156	SPECIAL CIRCUMSTANCES.....	100
157	Security Incidents Involving Deliberate Compromise, a Foreign Intelligence Service or a	
158	Terrorist Organization.....	100
159	Security Incidents Involving Apparent Violations of Criminal Law.....	101
160	Security Incidents Involving COMSEC or Cryptologic Information.....	101
161	Security Incidents Involving SCI.....	101
162	Security Incidents Involving RD and/or FRD.....	101
163	Security Incidents Involving IT.....	101
164	Security Incidents Involving FGI or NATO Information.....	101
165	Security Incidents Involving Classified U.S. Information Provided to Foreign	
166	Governments.....	102
167	Security Incidents Involving SAPs.....	102
168	Security Incidents Involving Improper Transfer of Classified Information.....	102
169	Security Incidents Involving On-Site Contractors.....	102
170	Security Incidents Involving Critical Program Information (CPI).....	103
171	Security Incidents Involving ACCM-Protected Information.....	103
172	Absence without Authorization.....	103
173	Coordination with Legal Counsel and the Department of Justice (DoJ).....	103
174	SECURITY INQUIRIES AND INVESTIGATIONS.....	103
175	Requirement.....	103
176	Coordination with Criminal Investigative Organization or Defense CI Component.....	103
177	Coordination with OCA.....	104
178	Security Inquiries.....	104
179	Security Investigations.....	106
180	INFORMATION APPEARING IN THE PUBLIC MEDIA.....	106
181	RESULTS OF INQUIRIES AND INVESTIGATIONS.....	108
182	ACTIONS TO BE TAKEN BY THE OCA.....	109
183	DAMAGE ASSESSMENTS.....	109
184	VERIFICATION, REEVALUATION, AND DAMAGE ASSESSMENT TIME LINES.....	110
185	ACTUAL OR POTENTIAL COMPROMISES INVOLVING MORE THAN ONE	
186	AGENCY.....	110
187	DEBRIEFING IN CASES OF UNAUTHORIZED ACCESS.....	111
188	REPORTING AND OVERSIGHT MECHANISMS.....	111
189		
190	APPENDIX 1 TO ENCLOSURE 6: SECURITY INCIDENT REPORTING FORMAT.....	113
191	APPENDIX 2 TO ENCLOSURE 6: DOJ MEDIA LEAK QUESTIONNAIRE.....	115
192	*(Added)(DAF) APPENDIX 3 TO ENCLOSURE 6: SECURITY INCIDENT TRACKER.	116
193		
194	ENCLOSURE 7: IT ISSUES FOR THE SECURITY MANAGER.....	118
195		
196	OVERVIEW.....	118

197	RESPONSIBILITY.....	118
198	IA ROLES AND FUNCTIONS.....	118
199	IA CONCEPTS.....	118
200	IA Attributes.....	118
201	System Categorization.....	119
202	Assessment and Authorization (A&A).....	119
203	DATA SPILLS.....	120
204	DISPOSAL OF COMPUTER MEDIA.....	121
205	NON-TRADITIONAL WORK ENVIRONMENTS.....	122
206	REQUIREMENT FOR ENCRYPTION OF CERTAIN UNCLASSIFIED DATA.....	123
207	PII.....	123
208	NEW TECHNOLOGY AND EQUIPMENT.....	123
209	INTERNET-BASED SOCIAL NETWORKING SERVICES.....	123
210	MARKING REQUIREMENTS FOR ELECTRONIC INFORMATION.....	124
211	PROCESSING REQUIREMENTS FOR SPECIFIC TYPES OF INFORMATION.....	124
212	SCI.....	124
213	RD and Critical Nuclear Weapons Design Information (CNWDI).....	124
214	SAP.....	124
215	Controlled Imagery.....	124
216	NATO Information.....	125
217	CUI.....	125
218	COMPILATION AND DATA AGGREGATION.....	125
219		
220	GLOSSARY.....	126
221		
222	PART I. ABBREVIATIONS AND ACRONYMS.....	126
223	PART I.A. *(Added)(DAF) ACRONYMS	128
224	PART II. DEFINITIONS.....	129
225		
226	FIGURES	
227	1. Conditions Governing Access to Official Records for Research Historical Purposes.....	21
228	2. Report of Security Incident Inquiry or Investigation.....	114
229		
230		
231		
232		
233		
234		
235		
236		

REFERENCES

237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280

- (a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended
- (b) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," April 21, 2016, as amended
- (c) DoD 5200.1-R, "Information Security Program," January 14, 1997 (cancelled by Volume 1)
- (d) Executive Order 13526, "Classified National Security Information," December 29, 2009
- (e) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010
- (f) Part 2001 of title 32, Code of Federal Regulations
- (g) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, "Revised Alternative Compensatory Control Measures (ACCM) Guidance," April 18, 2003 (hereby cancelled)
- (h) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, "Classified Information at Meetings and Conferences," October 26, 2001 (hereby cancelled)
- (i) DoDM 5105.21, Volume 1, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security," October 19, 2012, as amended
- (j) DoDM 8910.01, "DoD Information Collections Manual: Procedures for Management of Internal Information Collections," June 30, 2014, as amended
- (k) DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019
- (l) DoDM 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017
- (m) DoD Instruction 5400.04, "Provision of Information to Congress," March 17, 2009
- (n) Department of Defense/Government Printing Office Security Agreement, 1981¹
- (o) DoD Instruction 7650.01, "Government Accountability Office (GAO) and Comptroller General Requests for Access to Records," January 27, 2009, as amended
- (p) DoD Directive 5405.2, "Release of Official Information in Litigation and Testimony by DoD Personnel as Witnesses," July 23, 1985
- (q) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
- Committee on National Security Systems Instruction 4004, "Destruction and Emergency
- (r) Protection Procedures for COMSEC and Classified Material," August 2006²
- (s) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended
- (t) Chapters 22 and 33 of title 44, United States Code
- (u) DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended
- (v) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended
- (w) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended

281 ¹ Contact Security Directorate, Office of the Deputy Under Secretary of Defense for Security and Intelligence
282 ² Documents issued by the Committee on National Security Systems (CNSS) are available at www.cnss.gov/full-index.html

283
284 (x) Parts 120 through 130 of title 22, Code of Federal Regulations (also known as "The

- 285 International Traffic in Arms Regulations”)
- 286 (y) DoD Directive 5230.11, “Disclosure of Classified Military Information to Foreign
287 Governments and International Organizations,” June 16, 1992
- 288 (z) DoD Instruction O-2000.16, “DoD Antiterrorism (AT) Program Implementation,” November
289 17, 2016, as amended
- 290 (aa) DoD Instruction 5240.05, “Technical Surveillance Countermeasures (TSCM) Program,” April
291 3, 2014, as amended
- 292 (ab) United States Security Authority for NATO Affairs Instruction 1-07, “Implementation of
293 NATO Security Requirements,” April 5, 2007³
- 294 (ac) Department of Defense and United Kingdom Ministry of Defense, “Security Implementing
295 Arrangement,” January 27, 2003⁴
- 296 (ad) Chairman of the Joint Chiefs of Staff Manual 3150.29C, “Code Word, Nickname, and
297 Exercise Terms Report (NICKA) System,” December 7, 2007⁵
- 298 (ae) DoD Directive 5000.01, “The Defense Acquisition System,” May 12, 2003, as amended
- 299 (af) Chairman of the Joint Chiefs of Staff Manual 5720.01B, “Joint Staff Message Management
300 and Preparation,” February 15, 2005⁶
- 301 (ag) DoD Directive 5205.07, “Special Access Program (SAP) Policy,” July 1, 2010, as amended
- 302 (ah) DoD Directive 5210.56, “Arming and the Use of Force,” November 18, 2016
- 303 (ai) DoD Instruction 3224.03, “Physical Security Enterprise and Analysis Program (PSEAP),” June
304 4, 2020
- 305 (aj) Federal Specification FF-L-2740, “Locks, Combination,” current edition⁷
- 306 (ak) Federal Standard 832, “Construction Methods and Materials for Vaults,” September 1, 2002⁷
- 307 (al) Federal Specification FF-L-2937, “Combination Lock, Mechanical,” January 31, 2005, as
308 amended⁷
- 309 (am) Federal Specification AA-F-358, “Filing Cabinet, Legal and Letter Size, Uninsulated,
310 Security,” current edition⁸
- 311 (an) Federal Specification AA-V-2737, “Modular Vault Systems,” April 25, 1990, with
312 Amendment 2, October 30, 2006⁷
- 313 (ao) Federal Specification FF-P-110, “Padlock, Changeable Combination (Resistant to Opening by
314 Manipulation and Surreptitious Attack),” current edition, as amended⁷
- 315 (ap) Section 1386 of title 18, United States Code
- 316 (aq) Federal Standard 809, “Neutralization and Repair of GSA-Approved Containers and Vault
317 Doors,” current edition⁷
- 318
- 319 ³ Available to authorized recipients from the Central U.S. Registry
- 320 ⁴ Contact the Director, International Security Programs, Defense Technology Security Administration, Office of the Under Secretary of Defense for
321 Policy
- 322 ⁵ Restricted distribution. Contact J-3, Office of the Joint Chiefs of Staff
- 323 ⁶ This document is available to authorized recipients at https://ca.dtic.mil/cjcs_directives/index.htm
- 324 ⁷ Available through DoD Lock Program at <https://locks.navfac.navy.mil> at the Documents, Federal Specifications tab for Federal Specifications or
325 Documents, Directives and Guidance tab for Federal Standards and Military Handbooks.
- 326
- 327
- 328 (ar) National Security Agency/Central Security Service Evaluated Product List 02-01, “NSA/CSS
329 Evaluated Products List for High Security Crosscut Paper Shredders” (also Annex A to

- 330 NSA/CSS Specification 02-01, “High Security Crosscut Paper Shredders”), current edition
 331 (as) National Security Agency/Central Security Service Evaluated Product List 02-02, “NSA/CSS
 332 Evaluated Products List for High Security Disintegrators” (also Annex A to NSA/CSS
 333 Specification 02-02, “High Security Disintegrators”), current edition
 334 (at) Military Handbook 1013/1A, “Design Guidelines for Physical Security of Facilities,”
 335 December 15, 1993⁸
 336 (au) Underwriters Laboratories Inc., Standard 634, “Standard for Connectors and Switches for Use
 337 with Burglar-Alarm Systems,” October 12, 2007⁹
 338 (av) National Security Agency/Central Security Service Policy Manual 3-16, “Control of
 339 Communications Security (COMSEC) Material,” August 2005¹⁰
 340 (aw) Executive Order 13549, “Classified National Security Information Program for State, Local,
 341 Tribal, and Private Sector Entities,” August 18, 2010
 342 (ax) Committee on National Security Systems, National Security Telecommunications and
 343 Information Systems Security Instruction (NSTISSI) No. 7003, “Protective Distribution
 344 Systems (PDS),” December 13, 1996
 345 (ay) DoD Instruction 5200.33, “Defense Courier Operations,” June 30, 2011
 346 (az) DoDM 5220.22, Volume 2, “National Industrial Security Program: Industrial Security
 347 procedures for Government Activities,” August 1, 2018
 348 (ba) Chapter I of title 39, Code of Federal Regulations
 349 (bb) DoD Instruction 8523.01, Communications Security (COMSEC), April 22, 2008
 350 (bc) Intelligence Community Directive 503, “Intelligence Community Information Technology
 351 Systems Security Risk Management, Certification and Accreditation,” September 15, 2008¹¹
 352 (bd) Department of Defense Foreign Clearance Manual, September 5, 2011¹²
 353 (be) DoD Directive 5105.65, “Defense Security Cooperation Agency (DCSA),” October 26, 2012
 354 (bf) DoD Directive 8140.01, “Cyberspace Workforce Management,” August 11, 2015, as amended
 355 (bg) DoD Instruction 3305.13, “DoD Security Education, Training, and Certification,” February
 356 13, 2014, as amended
 357 (bh) DoD Instruction 5205.11, “Management, Administration, and Oversight of DoD Special
 358 Access Programs (SAPs),” February 6, 2013, as amended
 359 (bi) Section 2723 of title 10, United States Code
 360 (bj) Intelligence Community Directive 701, “Security Policy Directive for Unauthorized
 361 Disclosures of Classified Information,” March 14, 2007¹³
 362 (bk) Sections 102, 105, 552¹⁴ and 552a¹⁵ of title 5, United States Code

363
 364 ⁸ Available through GSA at [http://www.gsa.gov/portal/content/103856#Federal Specifications](http://www.gsa.gov/portal/content/103856#Federal%20Specifications)

365 ⁹ Available from Underwriters laboratories Inc. at <http://www.ul.com/global/eng/pages/solutions/standards> ¹⁰ Available to authorized recipients at
 366 www.iad.nsa.smil.mil/resources/library/nsa_office_of_policy_section/index.cfm

367 ¹¹ Available at http://www.dni.gov/electronic_reading_room/ICD_503.pdf

368 ¹² Available at <https://www.fcg.pentagon.mil>

369 ¹³ Available on JWICS at <http://www.intelink.ic.gov/sites/ppr/policyHome/default.aspx>

370 ¹⁴ Also known and referred to in this volume as “The Freedom of Information Act (FOIA),” as amended

371 ¹⁵ Also known and referred to in this volume as “The Privacy Act of 1974, as amended”

- 372
 373
 374 (bl) DoD Directive 5230.24, “Distribution Statements on Technical Documents,” August 23, 2012,
 375 as amended
 376 (bm) DoD Directive 5240.06, “Counterintelligence Awareness and Reporting (CIAR),” May 17,

- 377 2011
- 378 (bn) Committee on National Security Systems, National Security Telecommunications and
379 Information Systems Security Instruction (NSTISSI) No. 4003, “Reporting and Evaluating
380 COMSEC Incidents,” December 2, 1991¹⁶
- 381 (bo) Section 3161 of Public Law 105-261, “National Defense Authorization Act for Fiscal Year
382 1999,” as amended
- 383 (bp) DoD Directive 5240.02, “Counterintelligence,” March 17, 2015, as amended
- 384 (bq) DoD Directive 8000.01, “Management of the Department of Defense Information Enterprise
385 (DoD IE),” March 17, 2016, as amended
- 386 (br) Committee on National Security Systems Policy 18, “National Policy on Classified
387 Information Spillage,” June 2006¹⁶
- 388 (bs) Committee on National Security Systems Instruction 1001, “National Instruction on Classified
389 Information Spillage,” February 2008¹⁶
- 390 (bt) Assistant Secretary of Defense for Command, Control, Communications and Intelligence
391 Memorandum, “Disposition of Unclassified DoD Computer Hard Drives,” June 4, 2001
- 392 (bu) Assistant Secretary of Defense for Networks and Information Integration Memorandum,
393 “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and
394 Removable Storage Media,” July 3, 2007
- 395 (bv) Assistant Secretary of Defense for Networks and Information Integration Memorandum,
396 “Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information
397 (PII),” August 18, 2006
- 398 (bw) Director, Administration and Management Memorandum, “Safeguarding Against and
399 Responding to the Breach of Personally Identifying Information,” September 25, 2008
- 400 (bx) DoD Instruction 8170.01, “Online Information Management and Electronic Messaging,”
401 January 2, 20
- 402 (by) DoD Directive 8320.02, “Data Sharing in a Net-Centric Department of Defense,”
403 December 2, 2004
- 404 (bz) DoD Instruction 5210.02, “Access to and Dissemination of Restricted Data and Formerly
405 Restricted Data,” June 3, 2011, as amended
- 406 (ca) Deputy Secretary of Defense Memorandum, “Protection of NATO Classified Information
407 Stored, Processed or Transmitted in U.S. Communication and Information (CIS) Systems and
408 Networks,” September 8, 2000
- 409 (cb) Deputy Secretary of Defense Memorandum, “Web Site Administration,”
410 December 7, 1998
- 411 (cc) DoD Instruction 5200.39, “Critical Program Information (CPI) Identification and Protection
412 within Research, Development, Test, and Evaluation (RDT&E),” May 28, 2015, as amended
- 413 (cd) DoDD 5400.07, “DoD Freedom of Information Act Program,” April 5, 2019
- 414 (ce) Section 403 of title 50, United States Code (also known as “The National Security Act of
415 1947,” as amended
- 416 (cf) Executive Order 12333, “United States Intelligence Activities,” December 4, 1981, as
417 amended

418 ¹⁶ NTISSI and documents issued by the Committee on National Security Systems (CNSS) are available at www.cnss.gov/full-index.html

- 419
- 420 (cg) Section 2162 of title 42, United States Code (also known as “The Atomic Energy Act of
421 1954,” as amended
- 422 **(ch) (Added)(DAF) DAFI 33-360, “Publications and Forms Management,” December 1, 2015**
423 **(correction August 7, 2021)**

- 424 (ci) (Added)(DAF) AFI 33-322, "Records Management and Information Governance
425 Program," March 23, 2020
- 426 (cj) (Added)(DAF) AFMAN 16-101, "Security Cooperation (SC) and Security Assistance (SA)
427 Management", August 2, 2018
- 428 (ck) (Added)(DAF) DAFMAN 16-201, "Department of the Air Force Foreign Disclosure and
429 Technology Transfer Program," January 19, 2021
- 430 (cl) (Added)(DAF) DoD Manual 5200.02_AFMAN 16-1405, "Air Force Personnel Security
431 Program," August 1, 2018
- 432 (cm) (Added)(DAF) DoDM5220.22V2_AFMAN 16-1406V2, "National Industrial Security
433 Program: Industrial Security Procedures for Government Activities," May 8, 2020
- 434 (cn) (Added)(DAF) USD(I&S) Memorandum, "Derivative Classification Training," January
435 31, 2019
- 436 (co) (Added)(DAF) AFI 17-203, "Cyber Incident Handling," 16 March 2017
- 437 (cp) (Added)(DAF) The Office of the Under Secretary of Defense for Intelligence
438 memorandum, "Clarification of Automated Entry Control System Minimum
439 Requirements," of 23 October 2013
- 440 (cq) (Added)(DAF) Security Executive Agent Directive 8, "Temporary Eligibility," 18 May
441 2020.
- 442 (cr) (Added)(DAF) Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*,
- 443 (cs) (Added)(DAF) DoD 5105.38-M, *Security Assistance Management Manual (SAMM)*,
- 444 (ct) (Added)(DAF) DAFMAN 17-1302-O, *Communications Security (COMSEC) Operations*,
- 445 (cu) (Added)(DAF) AFI 71-101, *Criminal Investigations Program*,
- 446 (cv) (Added)(DAF) Security Executive Agent Directive 4

447
448

449 *(Added)(DAF) ADOPTED FORMS

- 450
- 451 (Added)(DAF) AF Form 310, *Document Receipt and Destruction Certificate*
- 452 (Added)(DAF) AF Form 847, *Recommendation for Change of Publication*
- 453 (Added)(DAF) AF Form 2427, *Lock and Key Control Register*
- 454 (Added)(DAF) AF Form 2583, *Request for Personnel Security Action*
- 455 (Added)(DAF) AF Form 2587, *Security Termination Statement*
- 456 (Added)(DAF) DD Form 254, *Department of Defense Contract Security Classification*
457 *Specification*
- 458 (Added)(DAF) Optional Form 89, *Maintenance Record for Security Containers/ Vault Doors*
- 459 (Added)(DAF) Standard Form (SF) 312, *Classified Information Nondisclosure Agreement*
- 460 (Added)(DAF) SF 700, *Security Container Information*
- 461 (Added)(DAF) SF 701, *Activity Security Checklist*
- 462 (Added)(DAF) SF 702, *Security Container Check Sheet*
- 463

ENCLOSURE 2

SAFEGUARDING

1. CONTROL MEASURES. DoD Components shall have a system of control measures that ensure access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which access occurs and to the nature and volume of the information. The system shall include technical, physical, and personnel control measures. Administrative control measures, which may include records of internal distribution, access, generation, inventory, reproduction, and disposition, shall be required when technical, physical, and personnel control measures are insufficient to deter and detect access by unauthorized persons. Except as otherwise specified, requests for waivers to the provisions of this Volume shall be submitted in accordance with section 16 of Enclosure 3 of Volume 1.

a. **(Added)(DAF) Waiver requests for access to collateral classified information shall be submitted through the MAJCOM/FLDCOM Information Protection (IP) directorate to the Director, Security, Special Program Oversight and Information Protection (SAF/AAZ), in accordance with Volume 1, of this Manual (T-0).**

b. **(Added)(DAF) Consistent with paragraph 2.7.3.8 of references (cj) and (ck), DAF system planning teams are responsible for surveying security protection of international transfers of classified information and CUI conducted via security cooperation efforts. (T-0). In addition, DAF programs must validate if the foreign partner or representative's has safeguarding capabilities in place to provide a commensurate level of protection that is substantially the same degree of protection as provided by the U.S. government (USG). (T-1).**

c. **(Added)(DAF) The commander or director (in coordination with the foreign disclosure officer and contact officer) hosting extended visits of foreign nationals/representatives, must review and approve the security plan prescribed by references (cj) and (ck). (T-1).**

2. PERSONAL RESPONSIBILITY FOR SAFEGUARDING. Everyone who works with classified information is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to classified information. Everyone granted access to classified information is personally responsible for protecting the classified information they know, possess, or control and for complying with the pre-publication security review processes specified in DoDD 5230.09 (Reference (k)). Classified information shall be protected at all times either by storing it as this Volume prescribes or by having it under the personal observation and control of an authorized individual.

3. ACCESS TO CLASSIFIED INFORMATION. Except as provided in sections 5 and 6 of this enclosure and in accordance with section 12 of Enclosure 3 of Volume 1, no person may have access to classified information unless that person has security clearance eligibility in accordance with DoDM 5200.02 (Reference (l)), has signed a Standard Form (SF) 312, "Classified Information Non-Disclosure Agreement (NDA)," and access is essential to the accomplishment of a lawful and authorized Government function (i.e., has a need-to-know).

513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561

a. ***(Added)(DAF)** The commander, vice commander or director will grant, suspend or remove access to classified information, for their subordinates, in accordance with DoD Manual 5200.02_AFMAN 16-1405, *Air Force Personnel Security Program*, (reference (c)) (this action may not be delegated any further). (T-0). Upon completion of the debriefing, the Defense Information Security System (DISS), or its successor system, must be updated. (T-0). The DoD Consolidated Adjudication Facility is the only entity who can suspend or revoke an individual's security clearance eligibility.

b. ***(Added)(DAF)** Prior to taking a servicing relationship with contractors in DISS, or successor system, and granting access to classified information, the security official will verify (or receive verification from the contracting officer's representative) that the accesses needed for disclosure of information under this contract are authorized, via a relevant DD Form 254. (T-1).

c. **(Added)(DAF)** The commander or director shall only grant U.S. personnel access to NATO information based on verification of final security clearance eligibility and a need-to-know. (T-0). This action may be delegated, in writing, when the commander or director is absent and at geographically separated units. Prior to granting access, the commander or director (or designated appointee) will:

(1) **(Added)(DAF)** Verify the individual has the proper final security clearance eligibility for the level of NATO information required. (T-0). Ensure DISS, or its successor system, is updated to reflect NATO access. (T-0).

(a) **(Added)(DAF)** For COSMIC top secret access, final U.S. top secret security clearance eligibility is required. (T-0).

(b) **(Added)(DAF)** For NATO secret and NATO confidential, final U.S. secret security clearance eligibility is required. (T-0).

(c) **(Added)(DAF)** For COSMIC top secret atomic information (ATOMAL) and NATO secret ATOMAL, final U.S. top secret security clearance eligibility is required as well as approved access to restricted data/formerly restricted data (RD/FRD). (T-0).

(d) **(Added)(DAF)** For NATO confidential ATOMAL, final U.S. secret security clearance eligibility is required as well as approved access to RD/FRD. (T-0).

(e) **(Added)(DAF)** For NATO restricted, security clearance eligibility is not required.

(2) **(Added)(DAF)** Use of the AF Form 2583, *Request for Personnel Security Action*, is optional.

(3) **(Added)(DAF)** Upon termination (regardless of type), the individual must be debriefed and DISS, or the successor system, must be updated, as noted in the AF Form 2587, *Security Termination Statement*. (T-1).

562 4. DETERMINING NEED FOR ACCESS. The individual with authorized possession,
563 knowledge, or control of the information has the final responsibility for determining whether a
564 prospective recipient's official duties requires them to possess or have access to any element or
565 item of classified information, and whether that prospective recipient has been granted the
566 appropriate security clearance by proper authority.

567
568
569 5. EMERGENCY AUTHORITY. In emergencies in which there is an imminent threat to life or in
570 defense of the homeland, the Heads of the DoD Components may authorize the disclosure of
571 classified information, including information normally requiring the originator's prior
572 authorization, to an individual or individuals who are otherwise not routinely eligible for access.

573
574 a. Limit the amount of classified information disclosed to the absolute minimum to achieve the
575 purpose.

576
577 b. Limit the number of individuals who receive classified information.

578
579 c. Transmit the classified information through approved Federal government channels by the
580 most secure and expeditious method consistent with this Volume, or by other means deemed
581 necessary when time is of the essence.

582
583 d. Provide instructions about what specific information is classified and how it should be
584 safeguarded. Information disclosed shall not be deemed declassified as of result of such disclosure
585 or subsequent use by a recipient. Physical custody of classified information must remain with an
586 authorized Federal government entity in all but the most extraordinary circumstances.

587
588 e. Provide appropriate briefings to the recipients on their responsibilities not to disclose the
589 information to unauthorized individuals and obtain a signed SF 312.

590
591 f. Notify the agency or DoD Component originating of the information and the Deputy Under
592 Secretary of Defense for Intelligence, and Security (DUSD(I&S)) within 72 hours of the disclosure
593 of classified information, or at the earliest opportunity that the emergency permits but no later than
594 30 days after the release.

595
596 (1) A description of the disclosed information.

597
598 (2) Identification of individuals to whom the information was disclosed.

599
600 (3) How the information was disclosed and transmitted.

601
602 (4) Reason for the emergency release.

603
604 (5) How the information is being safeguarded.

605
606 (6) A description of the briefings provided.

607
608 (7) A copy of the signed SF(s) 312.

609
610 g. ***(Added)(DAF) The cognizant DAF commander or director (or on-scene commander**

611 **in certain cases) may authorize the disclosure of classified information in emergencies where**
612 **there is an imminent threat to life (e.g., fire, major accident response, natural disaster).**
613 **Emergencies where there is an imminent threat to the defense of the homeland, the**
614 **installation or host wing commander may authorize the disclosure of classified information.**
615 **The disclosing authority shall complete all requirements listed in paragraph f. (above). (T-0).**
616
617

618 6. ACCESS BY INDIVIDUALS OUTSIDE THE EXECUTIVE BRANCH. Classified
619 information may be made available to individuals or agencies outside the Executive Branch, as
620 provided in this section, if such information is necessary for performance of a lawful and
621 authorized function, and such release is not prohibited by the originating department or agency.
622 The Heads of DoD Components shall designate officials to ensure the recipient's eligibility for
623 access, prior to the release of classified information (See Volume 1, Enclosure 3, section 11 for
624 requirements for access by individuals inside the Executive Branch).
625

626 a. Congress. DoDI 5400.04 (Reference (m)) provides rules for access to classified information
627 or material by Congress, its committees, members, and staff representatives. Members of
628 Congress, by virtue of their elected position, are not investigated or cleared by the Department of
629 Defense.
630

631 b. Government Printing Office (GPO). Collateral documents and material of all classifications
632 may be processed by the GPO, which protects the information according to a DoD/GPO Security
633 Agreement (Reference (n)).
634

635 c. Representatives of the Government Accountability Office (GAO). DoDI 7650.01
636 (Reference (o)) sets forth rules for granting GAO representatives access to classified information
637 that the Department of Defense originates and possesses when such information is relevant to the
638 performance of the statutory responsibilities of that organization. Certifications of security
639 clearances and the basis therefore, shall be accomplished under arrangements between the GAO
640 and the relevant DoD Component. Personal recognition or presentation of official GAO credential
641 cards are acceptable for identification purposes, but not for access to classified information.
642

643 d. Historical Researchers. Persons outside the Executive Branch who are engaged in historical
644 research projects may be authorized access to classified information provided that the DoD
645 Component Head or Senior Agency Official (SAO) with classification jurisdiction over the
646 information:
647

648 (1) Determines, in writing, that such access is clearly consistent with the interests of
649 national security in view of the intended use of the material to which access is granted by certifying
650 that the requester has been found to be eligible for access pursuant to Reference (l) and section 3 of
651 this enclosure.
652

653 (2) Limits access to specific categories of information over which the DoD Component
654 has classification jurisdiction or for which the researcher has the written consent of the DoD
655 Component or non-DoD agency with classification jurisdiction. The information contained within
656 or revealed by the specified categories must be within the scope of the research.
657

658 (3) Maintains custody of the classified material at a DoD installation or activity or
659 authorizes access to documents held by the National Archives and Records Administration

660 (NARA).

661

662 (4) Obtains the requester's agreement to safeguard the information and to submit any
663 notes and manuscripts intended for public release for review by all DoD Components or non-DoD
664 departments or agencies with classification jurisdiction to determine whether classified information
665 is contained therein. The agreement shall be documented by execution of a statement substantially
666 similar to that in Figure 1.

667

668 (5) Authorizes access, in writing, for no more than 2 years from the date of issuance. The
669 DoD Component may renew access for 2-year periods in accordance with DoD Component- issued
670 regulations.

671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723

Figure 1. Conditions Governing Access to Official Records by Historical Researchers

To Whom It May Concern:

I understand that the classified information to which I have requested access for historical research purposes is concerned with the national defense or foreign relations of the United States. Unauthorized disclosure could reasonably be expected to cause damage, serious damage, or exceptionally grave damage to the national security depending on whether the information is classified Confidential, Secret, or Top Secret, respectively. If granted access, I therefore agree to the following conditions governing access to the **[insert Component or activity]** files:

1. I will abide by any rules and restrictions issued in your letter of authorization, including those of other Agencies whose information is interfiled with that of the [insert Component or activity].
2. I agree to safeguard the classified information to which I gain possession or knowledge in a manner consistent with Part 4 of Executive Order 13526, "Classified National Security Information," and the applicable provisions of the DoD regulations concerning safeguarding classified information, including Volumes 1, 2, and 3 of DoD Manual 5200.01, "DoD Information Security Program."
3. I agree not to reveal to any person or Agency, classified information obtained because of this access except as authorized in the terms of your authorization letter or a follow-on letter. I further agree that I shall not use the information for purposes other than those set forth in my request for access.
4. I agree to submit my research notes for review to determine if classified information is contained in them before their removal from the specific area assigned to me for research. I further agree to submit my manuscript(s) for a security review before its publication or presentation. In each of these reviews, I agree to comply with any decision of the reviewing official in the interests of the security of the United States, including the retention or deletion of any classified parts of such notes and manuscript whenever the Federal Agency concerned deems such retention or deletion necessary.
5. I understand that failure to abide by the conditions in this statement shall constitute sufficient cause for canceling my access to classified information and for denying me any future access and may subject me to criminal provisions of Federal Law as referred to in Item 6.
6. I have been informed that provisions of title 18 of the United States Code impose criminal penalties, under certain circumstances, for the unauthorized disclosure, loss, copying, or destruction of defense information.

THIS STATEMENT IS MADE TO THE UNITED STATES GOVERNMENT TO ENABLE IT TO EXERCISE ITS RESPONSIBILITY FOR THE PROTECTION OF INFORMATION AFFECTING THE NATIONAL SECURITY. I UNDERSTAND THAT ANY MATERIAL FALSE STATEMENT THAT I MAKE KNOWINGLY AND WILLFULLY SHALL SUBJECT ME TO THE PENALTIES OF TITLE 18 OF THE U.S. CODE, SECTION 1001.

Researcher's Signature: _____
Witness's Signature: _____
Date: _____

724 e. Presidential or Vice Presidential Appointees and Designees. Persons who previously
 725 occupied senior policy-making positions to which they were appointed or designated by the
 726 President or Vice President may not remove classified information upon departure from office, as
 727 all such material shall remain under the U.S. Government's security control. Such persons may be
 728 authorized access to classified information they originated, reviewed, signed, received, or that was
 729 addressed to them while serving as an appointee or designee, provided that the DoD Component
 730 Head or senior agency official with classification jurisdiction for such information:

731
 732 (1) Determines, in writing, that such access is clearly consistent with the interests of
 733 national security in view of the intended use of the material to which access is granted and by
 734 certifying that the requester has been found to be eligible for access pursuant to section 3 of this
 735 enclosure.

736
 737 (2) Limits access to items that the person originated, reviewed, signed, or received while
 738 serving as a Presidential or Vice Presidential appointee or designee.

739
 740 (3) Retains custody of the classified material at a DoD installation or activity or authorizes
 741 access to documents in the custody of the NARA.

742
 743 (4) Obtains the requestor's SF 312 to safeguard the information and to submit any notes
 744 and manuscript for pre-publication review by all DoD Components and non-DoD departments or
 745 agencies with classification jurisdiction to determine that no classified information is contained
 746 therein.

747
 748 f. Use of Classified Information in Litigation. DoDD 5405.2 (Reference (p)) governs the use
 749 of classified information in litigation.

750
 751 g. Special Cases. When necessary in the interests of national security, the Heads of the DoD
 752 Components or their senior agency official may authorize access to classified information by
 753 persons outside the Federal government, other than those enumerated in section 5 of this enclosure
 754 and paragraphs 6.a through 6.f of this section. Prior to authorizing access, such official must
 755 determine that the recipient is reliable, loyal, and trustworthy for the purpose of accomplishing a
 756 national security objective; meets the requirements of section 3 of this enclosure; and can and will
 757 safeguard the information from unauthorized disclosure (UD). The national security objective shall
 758 be stated in the authorization, which shall be in writing. This authority may not be further
 759 delegated.

760
 761 h. ***(Added)(DAF) The authority and responsibility to grant temporary access, for**
 762 **paragraphs b. – g. (above) is now in accordance with the *Security Executive Agent Directive 8,***
 763 **of 18 May 2020 (or successor policy).**

764
 765
 766 7. VISITS. The Heads of the DoD Components shall establish procedures to accommodate visits
 767 to their Component facilities involving access to, or disclosure of, classified information. As a
 768 minimum, these procedures shall include verifying the identity, personnel security clearance, access
 769 (if appropriate), and need to know for all visitors.

770
 771 a. Visit requests shall be processed and security clearance and access level verified using the
 772 Joint Personnel Adjudication System (JPAS) (or successor system) for DoD civilian, military, and

773 contractor personnel whose access level and affiliation are reflected in JPAS (or successor system).
774 Fax, telephone or other appropriate method shall be used for those personnel whose access level
775 and affiliation are not reflected in JPAS (or successor system).

776
777 b. Visits by foreign nationals to DoD Components and facilities, except for activities or events
778 that are open to the public, shall be handled in accordance with DoDD 5230.20 (Reference (q)) and
779 documented in the Foreign Visits System Confirmation Module.

780
781 c. **(Added)(DAF) The commander or director shall establish procedures to accommodate**
782 **visits involving access to, or disclosure of, classified or controlled unclassified information.**
783 **(T-1).**

784
785
786 8. PROTECTION WHEN REMOVED FROM STORAGE. An authorized person shall keep
787 classified material removed from storage under constant surveillance. Classified document cover
788 sheets (SF 703, “Top Secret (Coversheet);” SF 704, “Secret (Coversheet);” or SF 705 “Confidential
789 (Coversheet)”) shall be placed on classified documents not in secure storage. The cover sheets
790 show, by color and other immediately recognizable format or legend, the applicable classification
791 level.

792
793
794 9. END OF DAY SECURITY CHECKS

795
796 a. The heads of activities that process or store classified information shall establish a system of
797 security checks at the close of each duty and/or business day to ensure that any area where
798 classified information is used or stored is secure. SF 701, “Activity Security Checklist,” shall be
799 used to record such checks. An integral part of the security check system shall be the securing of
800 all vaults, secure rooms, and containers used for storing classified material. SF 702, “Security
801 Container Check Sheet,” shall be used to record such actions. The SF 701 and 702 shall be retained
802 and disposed of as required by Component records management schedules.

803
804 b. ***(Added)(DAF) The SF 701 and SF 702 must be retained in accordance with Air Force**
805 **Records Information Management System (AFRIMS) Table 31-04, Rule 02.00 (or subsequent**
806 **revisions). (T-1). If the SF 701 or SF 702 is being used to support findings in a security**
807 **inquiry or investigation, retain until the inquiry or investigation has been closed. (T-0).**

808
809
810 10. EMERGENCY PLANS. Plans shall be developed to protect, remove, or destroy classified
811 material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to
812 minimize the risk of compromise, and for the recovery of classified information, if necessary,
813 following such events. The level of detail and the amount of testing and rehearsal of these plans
814 shall be determined by assessing the risk of hostile action, foreign intelligence threats, natural
815 disaster, or terrorist activity that may place the information in jeopardy.

816
817 a. Use the requirements of Committee on National Security Systems (CNSS) Instruction 4004
818 (Reference (r)) when developing plans for the emergency protection (including emergency
819 destruction under no-notice conditions) of classified communications security (COMSEC) material.

820
821 b. When preparing emergency plans, consider:

822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870

(1) Reducing the amount of classified material on hand.

(2) Storing less frequently used classified material at other secure locations.

(3) Creating regular backup copies of information in electronic formats for off-site storage.

(4) Transferring as much retained classified information to removable electronic media as possible, thereby reducing its bulk.

c. *(Added)(DAF) Emergency plans are required to be posted in all activity spaces that process or store classified information/material. (T-0). Ease of access is important, as activity personnel must be aware of their responsibilities to protect classified information during these types of conditions. A template is provided at appendix 2, of this enclosure, and contains the minimum emergency plan topics that must be covered. (T-1).

d. *(Added)(DAF) MAJCOM/FLDCOMs will require activities they service to maintain a consolidated emergency plan, with an annex for each organization under their cognizance. (T-1). The annex must be coordinated with all entities expected to support it, such as security forces or firefighting services. (T-1). Subordinate activities must also conduct an annual exercise, at minimum, to test the effectiveness of the emergency plans, and update the plan based-on the exercises' after action reports. (T-1). Periodicity will be determined by the servicing MAJCOM/FLDCOM IP office.

11. USE OF SECURE COMMUNICATIONS. In accordance with the requirements of Enclosure 4, classified information shall be transmitted only over secure communications circuits approved for transmission of information at the specified level of classification. This includes communication by telephone, facsimile, e-mail and other forms of electronic communications (e.g., messages, websites). See Volume 2 of this Manual for guidance on required markings.

12. REMOVAL OF CLASSIFIED INFORMATION FOR WORK AT HOME. When it is mission critical for individuals to remove classified information and materials (e.g., IT equipment and associated storage media) for work at home, specific security measures and approvals are required. Security measures appropriate for the level of classification must be in place to provide adequate protection and security-in-depth and to prevent access by unauthorized persons. Compliance with section 13 of Enclosure 4 of this Volume is also required.

a. Top Secret. Only the Secretary of Defense, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commanders, or the senior agency officials appointed pursuant to section 5.4(d) of Reference (d) may authorize the removal of Top Secret information from designated working areas for work at home. Such officials may also authorize removal of information for work at home for any lower level of classification.

b. Secret and Confidential. The Heads of the DoD Components may authorize removal of Secret and Confidential information from designated working areas for work at home. This authority shall not be delegated below the major command or equivalent level.

871 c. Residential Storage Equipment. A General Services Administration (GSA)-approved
872 security container shall be furnished for residential storage of classified information. Written
873 procedures shall be developed to provide for appropriate protection of the information, including a
874 record of the classified information that has been authorized for removal for work at home.
875

876 d. Classified IT Systems. See section 7 of Enclosure 7 of this Volume when classified IT
877 equipment will be used. All residential classified network connections must be certified and
878 accredited in accordance with DoDI 8510.01 (Reference (s)) requirements.
879

880 e. Foreign Country Restriction. Work at home may be authorized in foreign countries only
881 when the residence is in a specific location where the U.S. enjoys extraterritorial status (e.g., on the
882 embassy, chancery, or consulate compound) or on a U.S. military installation.
883

884 **f. (Added)(DAF) Top secret requests for residential storage shall be submitted by the**
885 **responsible MAJCOM/FLDCOM IP office to SAF/AAZ, at least 30 duty days in advance of**
886 **the requirement. (T-0).**
887

888 **g. (Added)(DAF) The MAJCOM/FLDCOM security program executive (SPE) shall**
889 **serve as the approval authority to allow command personnel to remove secret and**
890 **confidential information from designated working areas, for work at home. (T-1).**
891

892 **h. (Added)(DAF) The use (storage) of classified information and/or material in**
893 **government quarters must be approved in this same manner. (T-0).**
894
895

896 13. WORKING PAPERS. Working papers are documents (e.g., notes, drafts, prototypes) or
897 materials (e.g., printer ribbons, photographic plates), regardless of the media, created during
898 development and preparation of a finished product. Working papers and materials are not intended
899 or expected to be disseminated. Working papers and materials containing classified information
900 shall be:

901 a. Dated when created.
902
903

904 b. Marked with the highest classification of any information contained therein.
905

906 c. Safeguarded as required for the assigned classification.
907

908 d. Conspicuously marked "Working Paper" on the cover and/or first page of the document or
909 material (or comparable location for special types of media) in letters larger than existing text.
910

911 e. Destroyed in accordance with chapter 33 of title 44, U.S.C. (Reference (t)) as implemented
912 by DoDD 5015.2 (Reference (u)) and appropriate DoD Component implementing directives and
913 records schedules when no longer needed.
914

915 f. Marked and controlled the same way as this Manual requires for finished products of the
916 same classification when retained more than 180 days from date of origin (30 days for SAPs), filed
917 permanently, e-mailed within or outside the originating activity, or released outside the originating
918 activity, except as provided in paragraph 13.g. of this section.
919

920 g. Shared between action officers, either physically or electronically, without controlling them
921 as permanent documents only when:

922
923 (1) The working materials are shared informally (e.g., collaborative documents or
924 coordinating drafts) in the development process.

925
926 (2) Transfer or transmission of the material is via secure means and, if electronic, by means
927 other than e-mail.

928
929 (3) All copies held by other than the originator are marked and controlled as required for
930 finished products when retained more than 180 days of origin (30 days for SAPs). Consult with the
931 originator for correct markings.

932
933
934 14. EQUIPMENT USED FOR PROCESSING CLASSIFIED INFORMATION. The DoD has a
935 variety of non-COMSEC-approved equipment that is used to process classified information. This
936 includes copiers, facsimile machines, computers, and other IT equipment and peripherals, display
937 systems, and electronic typewriters. Activities shall identify those features, parts, or functions of
938 equipment used to process classified information that may retain all or part of the information.
939 Security procedures shall prescribe the appropriate safeguards to:

940
941 a. Prevent unauthorized access to that information, including by repair or maintenance
942 personnel.

943
944 b. Ensure that repair procedures do not result in unauthorized dissemination of or access to
945 classified information. Where equipment cannot be properly sanitized or appropriately
946 knowledgeable escort provided, cleared maintenance technicians shall be used. Electronic repair or
947 diagnostic equipment shall be maintained as classified material by the DoD Component if there is
948 the potential for classified data transmission from the equipment being serviced. Use of remote
949 diagnostic or repair capabilities shall be specifically approved and authorized in writing by the
950 activity security manager; if the equipment retains or stores any classified information appropriate
951 physical and logical protection must be provided on the remote end and secure communications are
952 required.

953
954 c. Replace and destroy equipment parts in the appropriate manner when classified information
955 cannot be removed. Removable disk drives, memory chips and boards, and other electronic
956 components of copiers, fax machines, etc. may be sanitized or destroyed in the same manner as
957 used for comparable computer equipment. Alternatively, the equipment shall be designated as
958 classified and be retained and protected accordingly.

959
960 d. Ensure that appropriately knowledgeable, cleared personnel inspect equipment and
961 associated media used to process classified information before the equipment is removed from
962 protected areas to ensure there is no retained classified information. Classification markings and
963 labels shall be removed from sanitized equipment and media after inspection, prior to removal from
964 protected areas.

965
966 e. Ensure computers and other equipment used to process classified information or to transmit
967 classified information across a network are certified and accredited in accordance with Reference
968 (s) as required by DoDD 8500.01E (Reference (v)). Measures to protect against compromising

969 emanations shall be implemented in accordance with DoDD C-5200.19 (Reference (w)).

970
971
972 15. REPRODUCTION OF CLASSIFIED MATERIAL. Paper copies, electronic files, and other
973 material containing classified information shall be reproduced only when necessary for
974 accomplishing the organization's mission or for complying with applicable statutes or Directives.
975 Use of technology that prevents, discourages, or detects unauthorized reproduction of classified
976 information is encouraged.

977
978 a. Unless restricted by the originating agency, top secret, secret and confidential information
979 may be reproduced, including by e-mailing, scanning, and copying, to the extent operational needs
980 require.

981
982 b. The DoD Components shall establish procedures that facilitate oversight and control of the
983 reproduction of classified information and the use of equipment for such reproduction, including
984 controls that ensure:

985
986 (1) Reproduction is kept to a minimum, consistent with mission requirements.

987
988 (2) Personnel reproducing classified information are knowledgeable of the procedures for
989 classified reproduction and aware of the risks involved with the specific reproduction equipment
990 being used and the appropriate countermeasures they are required to take.

991
992 (3) Reproduction limitations originators place on documents and special controls applicable
993 to special categories of information are fully and carefully observed.

994
995 (4) Reproduced material is placed under the same accountability and control requirements
996 as applied to the original material. Extracts of documents will be marked according to content and
997 may be treated as working papers if appropriate.

998
999 (5) Reproduced material is conspicuously identified as classified at the applicable level and
1000 copies of classified material are reviewed after the reproduction process to ensure that the required
1001 markings exist.

1002
1003 (6) Waste products generated during reproduction are protected and destroyed as required.

1004
1005 (7) Classified material is reproduced only on approved and, when applicable, properly
1006 accredited systems. Section 14 of this enclosure provides additional guidance.

1007
1008 (8) Foreign government information (FGI) is reproduced and controlled pursuant to
1009 guidance and authority granted by the originating government.

1010
1011
1012 16. CLASSIFIED MEETINGS AND CONFERENCES. Meetings and conferences involving
1013 classified information present special vulnerabilities to unauthorized disclosure. The Heads of the
1014 DoD Components shall establish specific requirements for protecting classified information at DoD
1015 Component-sponsored meetings and conferences, to include seminars, exhibits, symposia,
1016 conventions, training classes, workshops, or other such gatherings, during which classified
1017 information is disseminated.

1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066

a. DoD Component approval processes shall ensure that the following requirements are met:

(1) The meeting or conference serves a specified U.S. Government purpose.

(2) Use of other approved methods or channels for disseminating classified information or material are insufficient or impractical.

(3) The meeting or conference, or classified sessions thereof, takes place only at an appropriately cleared U.S. Government facility or a U.S. contractor facility that has an appropriate facility security clearance and, as required, secure storage capability, unless an exception is approved, in writing, in advance by the DoD Component Head or SAO. Such exception authority shall not be delegated below the SAO. Requests for exceptions to permit use of facilities other than appropriately cleared U.S. Government or U.S. contractor facilities shall be submitted to the DoD Component Head or senior agency official in accordance with Component procedures. The request shall include a security plan that describes how the requirements of paragraphs 16.b and 16.d of this section shall be met.

(a) If classified meetings or conferences occur at a cleared U.S. contractor location, the contractor shall comply with all applicable portions of DoD 5220.22-M (Reference (w)) and parts 120 through 130 of title 22, CFR (Reference (y)) (also known as “The International Traffic in Arms Regulations”). DoD approval to conduct the meeting does not constitute authorization for presentation of export-controlled information when foreign nationals attend.

(b) The conduct of classified meetings or conferences at foreign installations and contractor sites is often subject to the rules and regulations of the host country, thus presenting additional security risks. Prior to approval of the conduct of such meetings, the DoD Component shall obtain assurances, in writing, that the responsible foreign government will agree to use security measures and controls that are at least as stringent as those required by this Manual. The provisions of paragraph 16.d. also shall be satisfied. To this end, assistance can be provided by the Director, International Security Programs, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy (OUSD(P)).

(c) Routine day-to-day meetings and gatherings of DoD officials shall be conducted only at an appropriately cleared U.S. Government or contractor facility. Exceptions shall not be granted for routine meetings.

(d) The provisions of this section do not apply to operational meetings conducted in combat situations, classes conducted by DoD schools, or gatherings of personnel of a DoD Component and foreign government representatives or U.S. and/or foreign contractor representatives on a matter related to a specific U.S. Government contract, program, or project.

(e) *(Added)(DAF) Exception to policy requests shall be submitted through the servicing installation IP office, to the servicing installation MAJCOM/FLDCOM 120 calendar days in advance, at minimum. (T-1). The MAJCOM/FLDCOM will forward to SAF/AAZ, 30 duty days in advance, at minimum. (T-1). The security plan must comprehensively describe and address potential security issues as well as the proposed methods to mitigate the risk. (T-0). Rationale regarding why the classified meeting/conference cannot take place at a USG or cleared contractor facility must also be

1067 **included. (T-1).**

1068

1069 (4) Classified sessions are segregated from unclassified sessions.

1070

1071 (5) Access to the meeting or conference, or specific sessions thereof, where classified
1072 information may be discussed or disseminated is limited to persons who possess an appropriate
1073 security clearance and need to know.

1074

1075 (6) Any participation by foreign nationals or foreign representatives complies with
1076 requirements of Reference (q) and DoDD 5230.11 (Reference (z)) (e.g., the responsible U.S.
1077 Government foreign disclosure office(s) assures, in writing, that the information to be presented has
1078 been approved for disclosure to the represented foreign countries).

1079

1080 (7) Announcement of the meeting or conference is unclassified and limited to a general
1081 description of topics expected to be presented, names of speakers, logistical information, and
1082 administrative and security instructions.

1083

1084 (8) Procedures shall ensure that classified information, documents, recordings, audiovisual
1085 material, information systems, notes, and other materials created, distributed, or used during the
1086 meeting are controlled, safeguarded, and transported as provisions of this Manual require.
1087 Recording or taking notes, including notes on classified electronic devices, during classified
1088 sessions shall be permitted only when it is determined that such action is necessary to fulfill the
1089 U.S. Government purpose for the meeting.

1090

1091 (9) Information systems used during the meeting or conference to support creation or
1092 presentation of classified information shall meet all applicable requirements for processing
1093 classified information, including as appropriate considerations of technical security
1094 countermeasures (TSCM). Unclassified laptop computers, handheld information technologies (e.g.,
1095 portable electronic devices (PEDs)), and other similar devices shall not be used for note taking
1096 during classified sessions. Use of classified computers and other electronic devices shall be
1097 permitted only when needed to meet the intent of the meeting or conference and appropriate
1098 protection and TSCM requirements have been met.

1099

1100 **(10) *(Added)(DAF) Ensure meeting or conference attendees are aware of the**
1101 **portable electronic device (PED) requirements outlined in the approved security plan.**
1102 **Unapproved devices introduced into the meeting or conference will be handled in accordance**
1103 **with enclosure 6, of this Manual. (T-0).**

1104

1105 b. The DoD activity sponsoring a classified meeting or conference shall assign an official to
1106 serve as security manager for the meeting and be responsible for ensuring that, at a minimum, the
1107 following security provisions are met:

1108

1109 (1) Attendees are briefed on safeguarding procedures.

1110

1111 (2) Entry is controlled so that only authorized personnel gain entry to the area. Particular
1112 caution shall be taken to ensure that any individual who is not authorized to attend the classified
1113 session(s) is denied entry thereto.

1114

1115 (3) The perimeter is controlled to ensure unauthorized personnel cannot overhear classified

1116 discussions or introduce devices that would result in the compromise of classified information.

1117
1118 (4) Escorts are provided for uncleared personnel who are providing services to the meeting
1119 or conference (e.g., setting up food or cleaning) when classified presentations and/or discussions
1120 are not in session.

1121
1122 (5) Use of cell phones, PEDs, 2-way pagers, and other electronic devices that transmit is
1123 prohibited.

1124
1125 (6) Classified notes and handouts are safeguarded in accordance with Enclosure 3.

1126
1127 (7) Classified information is disclosed to foreign nationals only in accordance with the
1128 provisions of Reference (z).

1129
1130 (8) An inspection of the room(s) is conducted at the conclusion of the meeting or
1131 conference (or at the end of each day of a multi-day event) to ensure all classified materials are
1132 properly stored.

1133
1134 **(9) (Added)(DAF) Security incident reporting procedures. (T-1).**

1135
1136 c. Appropriately cleared U.S. Government contractor personnel may provide administrative
1137 support and assist in organizing a classified meeting or conference, but the DoD Component
1138 sponsoring the gathering remains responsible for all security requirements.

1139
1140 d. Facilities other than appropriately cleared U.S. Government or U.S. contractor facilities
1141 proposed for use for classified meetings and conferences shall:

1142
1143 (1) Not be open to the public and access shall be controlled by the U.S. Government or
1144 cleared contractor through a 100 percent identification card check at the perimeter point. For a
1145 military installation or comparably protected Federal government compound, this can be at the
1146 perimeter fence of the installation or compound.

1147
1148 (2) Have the room(s) where the classified sessions are to be held located away from public
1149 areas so that access to the room(s), walls, and ceiling(s) can be completely controlled during the
1150 classified sessions.

1151
1152 (3) Provide authorized means to secure classified information in accordance with Enclosure
1153 3, of this Volume.

1154
1155 (4) Meet the DoD antiterrorism standards specified by DoDI 2000.16 (Reference (aa)).

1156
1157 (5) Be subject to TSCM surveys in accordance with DoDI 5240.05 (Reference (ab)). When
1158 addressing this requirement, TSCM security classification guidance MUST be consulted to ensure
1159 proper classification of meeting details when associated with the use of TSCM.

1160
1161 e. Not later than 90 days following the conclusion of a classified meeting or conference for
1162 which an exception was granted, the sponsoring activity shall provide an after-action report to the
1163 OUSD(I&S) through the approving DoD Component Head or SAO. The after-action report shall
1164 be a brief summary of any issues or threats encountered during the event and actions taken to

1165 address the situation.

1166
1167
1168 17. SAFEGUARDING FGI

1169
1170 a. North Atlantic Treaty Organization (NATO) Information. NATO classified information
1171 shall be controlled and safeguarded according to United States Security Authority for NATO
1172 Instruction 1-07 (Reference (ac)).

1173
1174 b. Other FGI. See the Glossary for the definition of FGI.

1175
1176 (1) To avoid inadvertent disclosure, classified FGI shall be stored in a manner that will
1177 avoid the commingling with other classified material. For small volumes of material, separate files
1178 in the same vault, container, or drawer will suffice.

1179
1180 (2) FGI shall be re-marked, if needed, to ensure the protective requirements are clear. FGI
1181 may retain its original classification if it is in English. However, when the foreign government
1182 marking is not in English, or when the foreign government marking requires a different degree of
1183 protection than the same U.S. classification designation, a U.S. marking that results in a degree of
1184 protection equivalent to that required by the foreign government shall be applied. See Appendix 1
1185 to Enclosure 4 of Volume 2 of this Manual for comparable U.S. classification designations.

1186
1187 (3) U.S. documents containing FGI shall be marked as required by section 9 of Enclosure
1188 4 of Volume 2 of this Manual. The foreign government document or authority on which derivative
1189 classification is based must be identified on the "Derived from:" line, in addition to the
1190 identification of any U.S. classification authority. A continuation sheet should be used for multiple
1191 sources, if necessary. A U.S. document containing FGI cannot be declassified or downgraded
1192 below the highest level of FGI contained in the document without the written permission of the
1193 foreign government or international organization that originated the information.

1194
1195 (4) Security clearances issued by the U.S. Government are valid for access to classified
1196 FGI of a comparable level.

1197
1198 (5) The transmission of FGI within the U.S. among U.S. Government agencies and U.S.
1199 contractors and between U.S. contractors with a need-to-know must be in accordance with this
1200 Manual and Reference (x).

1201
1202 (6) The international transfer of foreign government classified information must be by
1203 government officials through government-to-government channels, or channels agreed upon in
1204 writing by the originating and receiving governments (collectively "government-to-government
1205 transfer"). See Enclosure 4 and its Appendix for further guidance on transfer of classified
1206 information.

1207
1208 (7) The receiving DoD Components shall protect FGI to at least a degree equivalent to that
1209 required by the foreign government or international organization that provided the information. FGI
1210 shall be controlled and safeguarded in the same manner as prescribed for U.S. classified
1211 information, except as described below. The control and safeguarding requirements for FGI may
1212 be modified as permitted by a treaty or international agreement, or, for foreign governments with
1213 which there is no treaty or international agreement, through formal written agreement between the

1214 responsible national security authorities or designated security authorities of the originating and
1215 receiving governments (hereafter referred to collectively as designated security authorities
1216 (DSAs)). The USD(P) serves as the DSA.

1217
1218 (a) Control of Foreign Government Top Secret Information. Maintain records for 5
1219 years of the receipt, internal distribution, destruction, annual inventory, access, reproduction, and
1220 transmittal of foreign government top secret information. Reproduction requires the consent of the
1221 originating government. Two-person authentication is required to destroy top secret FGI.

1222
1223 (b) Control of Foreign Government Secret Information. Maintain records for 3 years
1224 of the receipt, distribution, external dispatch, reproduction, and destruction of material containing
1225 foreign government secret information. Other records may be necessary if the originator requires.
1226 Secret FGI may be reproduced to meet mission requirements.

1227
1228 (c) Control of Foreign Government Confidential Information. Maintain records for 2
1229 years for the receipt and external dispatch of confidential FGI. Do not maintain other records for
1230 foreign government confidential information unless required by the originating government.
1231 Confidential FGI may be reproduced to meet mission requirements.

1232
1233 (d) Foreign Government Restricted Information and Information Provided in
1234 Confidence. In order to ensure the protection of Restricted FGI or foreign government unclassified
1235 information provided in confidence, such information shall be classified in accordance with
1236 Reference (d) which states that unauthorized disclosure of FGI is presumed to cause damage to the
1237 national security. If the foreign protection requirement is lower than the protection required for
1238 U.S. confidential information, the information shall be marked "CONFIDENTIAL-Modified
1239 Handling" as described in Volume 2, Enclosure 4, paragraph 4.c of this Manual and the following
1240 requirements shall also be met:

1241
1242 1. The information shall be provided only to those individuals who have an
1243 established need to know, and where access is required by official duties.

1244
1245 2. Individuals given access shall be notified of applicable handling instructions.
1246 This may be accomplished by a briefing, written instructions, or by applying specific handling
1247 requirements to an approved coversheet.

1248
1249 3. Documents shall be stored to prevent unauthorized access (e.g., a locked desk
1250 or cabinet or a locked room to which access is controlled).

1251
1252 4. DoD Components and contractors performing on DoD contracts shall handle
1253 documents bearing the marking "UK RESTRICTED" as classified in accordance with
1254 subparagraph 17.b.(7)(d). The provision in the U.S./United Kingdom (UK) Security Implementing
1255 Arrangement (Reference (ad)) that allows documents marked "UK RESTRICTED" to be handled
1256 in a manner similar to For Official Use Only (FOUO) information applies ONLY to DoD
1257 contactors operating under COMMERCIAL contracts with the UK and, pursuant to the agreement,
1258 the UK must include in the applicable contract its requirements for the marking and handling of the
1259 information. The provision does NOT apply to, nor permit, such handling of UK RESTRICTED
1260 information by DoD Components or by contractors when performing on DoD contracts.

1261
1262 (8) FGI shall not be disclosed to nationals of third countries, including foreign

1263 nationals who are protected individuals or permanent resident aliens, or to any other third party, or
1264 used for other than the purpose for which the foreign government provided it without the
1265 originating government's written consent. Questions regarding releasability or disclosure should be
1266 directed to the U.S. originator, who will consult with the foreign government as required.
1267 Contractors will submit their requests through the contracting U.S. Government agency for U.S.
1268 contracts and the DCSA for direct commercial contracts. Approval from the originating
1269 government does not eliminate the requirement for the contractor to obtain an export authorization
1270 as required by other regulations or policies.

1271
1272
1273 18. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM). A Head of a DoD
1274 Component with original classification authority (OCA) may employ ACCM when he or she
1275 determines that the standard security measures detailed in this Manual are insufficient to enforce
1276 need-to-know for classified information and SCI or SAP protections are not warranted. The use of
1277 an unclassified nickname, obtained in accordance with Chairman of the Joint Chiefs of Staff
1278 Manual (CJCSM) 3150.29C (Reference (ae)), together with a list of persons authorized access, and
1279 a specific description of information subject to the enhanced ACCM controls, are the three requisite
1280 elements of an ACCM.

1281
1282 a. DoD Proponents for ACCM. The DoD staff proponent for ACCM management, oversight
1283 and Congressional reporting is the OUSD(P). The proponent for ACCM security policy is the
1284 OUSD(I&S). Given this sharing of ACCM responsibilities, staff elements in OUSD(P) and
1285 OUSD(I&S) shall implement mechanisms that ensure transparency of all ACCM actions.

1286
1287 b. ACCM Approval. A Head of a DoD Component may approve ACCM use for classified
1288 information over which they have cognizance. Prior to approving the establishment of an ACCM,
1289 the criticality, sensitivity, and value of the information; analysis of the threats both known and
1290 anticipated; vulnerability to exploitation; and a countermeasures cost benefits analysis shall be
1291 assessed.

1292
1293 c. Guidance on ACCM Use. Use of ACCM must be consistent with the following guidance:

1294
1295 (1) ACCM may be used to assist in enforcing need-to-know for classified DoD
1296 intelligence matters. The DoD Component Head establishing or terminating any such ACCM shall
1297 provide written notification within 30 days to the Director of Security, OUSD(I&S), and the
1298 Director, Special Programs, OUSD(P), who shall maintain this information as long as the ACCM is
1299 in use.

1300
1301 (2) ACCM may be used to assist in enforcing need to know for classified operations,
1302 sensitive support, and other non-intelligence activities. The DoD Component Head establishing or
1303 terminating any such ACCM shall provide written notification within 30 days to the Director,
1304 Special Programs, OUSD(P), for review. The Director, Special Programs, OUSD(P), shall
1305 maintain this information as long as the ACCM is in use.

1306
1307 (3) ACCM shall not be used for acquisition programs or activities progressing through the
1308 acquisition process.

1309
1310 (4) DoD Components shall obtain an unclassified nickname consistent with Reference (ae)
1311 and coordinate with OUSD(P) to preclude duplication of nicknames.

1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360

(5) A roster or listing of all persons accessed to the ACCM shall be maintained by the ACCM control officer (see subparagraph 18.f.(1)(c) of this section). The access roster will differentiate between those persons actively accessed and those whose accesses are currently inactive.

(6) ACCM documents and materials shall be marked as specified in Enclosure 4 of Volume 2 of this Manual.

(7) Heads of DoD Components must establish and maintain a system that provides for recurrent inspection of the ACCM they have approved. This mechanism shall ensure compliance with the provisions of this Manual. Each ACCM shall be overseen and inspected on a recurrent basis by the ACCM sponsor or OUSD(P).

d. Prohibited Security Measures. The application of the following security measures with ACCM material is prohibited:

(1) Using personnel security investigative or adjudicative standards that are more stringent than those normally required for a comparable level of classified information to establish access eligibility to ACCM-protected information.

(2) Using code words as defined in Reference (ae).

(3) Using trigraphs, digraphs, or other abbreviations of the approved nickname.

(4) Using specialized non-disclosure agreements or any certificates of disclosure or non-disclosure for ACCM access.

(5) Using a billet structure or system to control the position or numbers of persons afforded ACCM access.

e. Prohibited Uses of ACCM. The following uses of ACCM are prohibited:

(1) Using ACCM for NATO or non-intelligence FGI. For NATO, exceptions to this limitation can be granted only by the Secretary of Defense. For non-intelligence FGI, exceptions to this limitation can be granted only by the USD(P). Request for exceptions shall be forwarded to the Director, International Security Programs, Defense Technology Security Administration, USD(P), for action. Such approvals must be documented and retained by the sponsor.

(2) Using ACCM to protect classified information in acquisition programs as defined in DoDD 5000.01 (Reference (DAF)).

(3) Using ACCM to protect technical or operational requirements of systems in the acquisition process. Systems in operational use are not viewed as being in the acquisition process. Components of operational systems are fielded end items, not items in the acquisition process, and improvements to fielded items are eligible for ACCM status if properly justified.

(4) Using ACCM to protect Restricted Data (RD), Formerly Restricted Data (FRD), COMSEC, SCI, SAP, or Nuclear Command and Control Extremely Sensitive Information.

1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409

(5) Using ACCM to protect unclassified information.

(6) Using ACCM to preclude or impede congressional, OSD, or other appropriate oversight of programs, command functions, or operations.

(7) Using ACCM to justify funding to procure or maintain a separate ACCM communication system.

f. Documentation

(1) Use of ACCM must be approved in writing by the cognizant DoD Component Head. The correspondence establishing the ACCM shall be signed by the DoD Component Head and shall include the following information:

(a) Unclassified nickname assigned in accordance with Reference (ae).

(b) Designation of the ACCM sponsor. As a minimum, the sponsor shall be a general or flag officer, or senior executive equivalent, who has OCA at the level of or higher than the information protected by the ACCM.

(c) Designation of an ACCM control officer who shall be the organization's point of contact for all matters concerning the ACCM. Subsequent changes in designated personnel shall be provided, in writing, to the Special Programs Office, USD(P).

(d) Description of the essential information to be protected by the ACCM.

(e) Effective activation date and expected ACCM duration.

(f) Any planned participation by foreign partners.

(2) The ACCM sponsor shall develop and distribute a program security plan, security classification guide, and program participant briefing to all participating organizations prior to the activation of the ACCM. As a minimum, the briefing will address the specific information that is subject to ACCM security measures.

(3) The Special Programs Office, USD(P), shall maintain a central repository of records for all DoD ACCM.

g. Annual Reports of ACCM Use. Not later than December 15 of each year, the DoD Components shall provide a report to USD(P) on all ACCM usage during the previous year. The exact format for this report shall be provided annually by USD(P), however, the general data elements include: ACCM nickname; purpose and/or description of the ACCM program; expected duration; and ACCM sponsor and ACCM control officer(s).

h. Sharing ACCM-Protected Information. ACCM-protected information may be shared with other DoD Components and/or other Federal government departments and agencies only when the recipient organization agrees to abide by the ACCM security requirements stipulated in this enclosure.

1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458

i. Contractor Access to ACCM. DoD contractors may participate in ACCMs, or be directed to participate, only when such access and the associated security plan are identified in the DD Form 254, "Contract Security Classification Specification." Care must be taken to ensure identification of the security plan does not disclose ACCM-protected data.

j. Program Maintenance

(1) ACCM sponsors shall maintain an updated listing of primary and alternate ACCM control officers for each organization to which they have extended their program.

(2) Each organization's ACCM control officer shall maintain an updated ACCM access control list for their organization.

(3) Initial contact between organizations will be between each organization's ACCM control officers. ACCM control officers may authorize action officer to action officer contact once access control lists have been exchanged between organizations.

(4) Personnel requiring access to ACCM-protected information shall receive specialized training upon initial access to the program and annually thereafter. Training, as a minimum, shall address the procedures for access, control, transmission, storage, and marking. Individuals may be required to sign an acknowledgement of training should the security plan so specify.

(5) ACCM documentation (i.e., program security plan and security classification guide) must be updated a minimum of once every 5 years.

(6) ACCM sponsors shall provide the following information, through the DoD Component Head, to USD(P) concurrently with the ACCM annual report:

(7) A listing of primary and alternate ACCM control officers for each organization managing an ACCM.

(8) Any updated ACCM documentation or confirmation that program documentation has been reviewed and is current.

k. Safeguarding ACCM Information. The provisions of this Manual regarding the safeguarding of classified information are modified with respect to use of ACCM as follows:

(1) Top secret, secret, and confidential coversheets (i.e., SFs 703, 704, and 705, respectively) used to cover ACCM material shall be over stamped or marked with "ACCM" and the appropriate nickname. Coversheets specifically designated by the DoD Components for use with ACCM must be approved by the Director of Security, USD(I&S), prior to use.

(2) ACCM material should be handled and stored based on the security classification of the information contained therein and in a manner that separates it from non-ACCM classified information. Separate GSA-approved storage containers are not required so long as everyone with access to container is also approved for access to the ACCM material stored within, but the measures used (e.g., segregated files, separate folders, drawers labeled for ACCM) shall prevent the commingling of ACCM material with other classified documents.

1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507

(3) ACCM information shall be transmitted in the same manner as other classified information at the same classification level with the following exceptions:

(4) ACCM information packaged for transmission shall have the inner envelope marked with the appropriate classification, the caveat "ACCM," and the assigned nickname, and shall be addressed to the attention of an individual authorized access to the ACCM information.

(5) The ACCM nickname shall be used in the text of message traffic and on cover sheets accompanying secure facsimile transmissions to assist in alerting the recipient that the transmission involves ACCM-protected information. Senders shall ensure that an authorized recipient is awaiting the transmission when sending via secure facsimile. When using the Defense Message System (DMS), the material must also be marked as "SPECAT" (Special Category) in accordance with the requirements and procedures in CJCSM 5720.01B (Reference (ag)). Due to limits in DMS processing, only one ACCM nickname should be used in a DMS message.

(6) Automated information systems or electronic files containing ACCM protected information shall be configured with appropriate discretionary access controls to ensure that access is restricted to individuals with authorized access.

(7) Secret Internet Protocol Router Network (SIPRNET) or other secure transmission methods authorized for processing information at the required level of classification may be used to transmit ACCM information. Each such transmission must be marked with the caveat "ACCM" and the authorized nickname in accordance with the marking guidance in Volume 2 and transmitted only to those authorized access to the ACCM information.

(8) The method of transmission selected for ACCM information, whether in hardcopy or electronic form, shall be consistent with the security classification assigned. Designation of information as requiring ACCM protection does not, in and of itself, require the transmission of the information by methods usually reserved for a higher level of classified information.

1. Security Incidents. Compromise of ACCM program information can present an immediate and real threat to national security and those personnel involved in mission execution. Anyone finding ACCM material out of proper control shall take actions to safeguard the material and shall immediately notify the local ACCM control officer, if known, or the local security manager.

(1) All reporting, inquiry, investigation, and damage assessment will be conducted per the guidelines contained in Enclosure 6 of this Volume. Any reports containing ACCM information shall be handled in accordance with the requirements of this Manual as modified by this section.

(2) Section 13 of Enclosure 6 of this Volume states the actions to take if unauthorized personnel are inadvertently afforded access to ACCM information. Inadvertent disclosure forms, commonly used with compartmented information, are not authorized for use with ACCM information.

(3) Because ACCM program information is not SCI or SAP, reasonable risk management procedures should be followed when ACCM program information is incorrectly placed on non-approved electronic processing systems or electronically transmitted to non-authorized personnel and/or systems. Deleting the file or material from all affected systems is normally a sufficient

1508 action unless the material in question is classified at a higher level of classification than that for
1509 which the system is accredited.

1510

1511 (4) The ACCM sponsor should be notified when the local inquiry and investigation is
1512 completed. Resolution will be in accordance with current guidance contained in Enclosure 6 of this
1513 Volume and must consider the guidance contained in the ACCM program security plan.

1514 Responsibility for the damage assessment remains with the ACCM sponsor. Any additional action
1515 will be as directed by the ACCM sponsor and the local security manager.

1516

1517 m. ACCM Termination. ACCM shall be terminated by the establishing DoD Component
1518 when ACCM security measures are no longer required. Notification of ACCM termination must be
1519 submitted, in writing, as required by paragraphs 18.c.(1) and 18.c.(2) of this enclosure.

1520

1521 n. Transitioning an ACCM to a SAP. If, at any point in time, the DoD Component Head
1522 determines that information protected by ACCM requires further protection as a SAP, authorization
1523 to establish a DoD SAP must be requested in accordance with DoD Directive 5205.07 (Reference
1524 (ah)).

1525

1526 o. ***(Added)(DAF) SAF/AAZ only provides administrative oversight for ACCM policy**
1527 **within the DAF. However, the DAF does not have, nor does it establish ACCM. DAF**
1528 **personnel supporting another activity's ACCM must abide by the security requirements**
1529 **provided by the cognizant ACCM sponsor, in accordance with volume 3, enclosure 2 of**
1530 **this Manual. (T-0).**

1531

1532 Appendix

1533 ***(Added)(DAF) Classified Meeting Checklist**

1534 ***(Added)(DAF) Emergency Plan Example**

***(Added)(DAF) APPENDIX 1 TO ENCLOSURE 2, CLASSIFIED MEETING CHECKLIST**

Classified Meeting Checklist				
The security assistant is responsible for ensuring all items below are accomplished, unless the commander or director has delegated the responsibility to another individual.				
<i>Note: In this instance, "meeting" encompasses briefings, conferences, etc.</i>				
#	Preparation Checks	Complete		Comments
		Yes	No	
1	Determine the highest level of classification to be disclosed, to include any additional access requirements			
2	Determine meeting location (e.g., USG or cleared contractor facility) Be sure to select a meeting location that provides good physical control of the meeting room and provides protection from unauthorized audio and visual disclosure			
3	Determine if entire meeting will be classified or if there will be unclassified breakout sessions			
4	Determine where classified material will be stored before, during and after the meeting and who will be responsible for managing it; this includes determining if classified note taking will be permitted and storage/distribution protocols			
5	Identify potential attendees; this includes determining if foreign nationals/representatives will be in attendance. If so, arrange for a disclosure review, of unclassified and classified information, from the foreign disclosure office			
6	Ensure a visit authorization request is submitted, for each attendee, in DISS (or successor system), to verify security clearance eligibility and establishment of need-to-know			
7	Establish a method to identify attendees for entry/reentry (e.g., control rosters, badges, etc.) into the meeting			
8	Establish a screening process for personal items (e.g., briefcases, backpacks, purses, etc.) to prevent unauthorized items from entering the meeting			
9	Identify information systems or audio equipment to be used and ensure it is authorized for classified disclosures			
10	Identify any special communication requirements (e.g., secure terminal equipment), if required			
#	Pre-meeting Inspection	Complete		Comments
		Yes	No	
1	If unfamiliar with building (meeting location), request the building manager be present while conducting walkthroughs			
2	Conduct a visual check of walls, ceilings, and floors for suspicious objects, accessible areas (e.g., holes, openings, exposed wires, etc.)			
3	Ensure all doors, windows and other openings are closed before disclosing classified information; first-floor windows and windows on doors must be covered to prevent visual disclosure; and windows on other floors that allow visual disclosure must be covered			
4	Check, touch and lift (if possible) the following items for things out of the ordinary (e.g., recording devices): Trash			

	containers, fire extinguishers, tables, desks, chairs, curtains, pictures, and circuit breaker panels			
#	Before/During the Meeting	Complete		Comments
		Yes	No	
1	Post appropriately cleared DAF personnel outside the meeting area, place signage on the doors, and/or lock entrances to control access			
2	Conduct sound checks to ensure conversations cannot be heard by un-cleared personnel outside the meeting area			
3	Conduct checks of personal items and look for unauthorized, unusual or suspicious items; if an attendee denies the inspection, the item shall not accompany the attendee past the entry control point			
4	Ensure portable electronic devices are not brought into areas where classified information is disclosed			
5	If classified note taking is permitted, brief attendees on the proper safeguarding and marking requirements prior to the start of the meeting			
6	Always announce the highest level of classification for each session			
7	Remind attendees that classified information cannot be discussed freely once the meeting is finished and discussions outside the designated area are prohibited			
8	Ensure all classified meeting material is properly marked and the appropriate coversheets are being utilized			
9	Employ procedures to protect classified material during any type of break, by establishing procedures for protection and storage of classified material at all times			
10	Revalidate all attendees upon reentry from breaks			
#	After the Meeting	Complete		Comments
		Yes	No	
1	Check all areas for unattended classified or unauthorized items left behind by attendees			
2	Notify the activity security manager or servicing information protection office of any security incidents			
3	Turn facility back over to facility manager, if required			
4	Ensure all classified material is secured in an authorized security container			
5	Ensure completed checklist is signed and dated			
Meeting Point of Contact		Signature		Date

***(Added)(DAF) APPENDIX 2 TO ENCLOSURE 2, EMERGENCY PLAN EXAMPLE**

1. Purpose. To establish procedures for the protection, removal and/or destruction of classified material located in building _____, room _____, on [installation]. These procedures will be executed in case of emergency, such as fire, natural disaster, civil disturbance, terrorist activities, or enemy attack.

2. Background

a. Each activity authorized to process or store classified information must develop an emergency plan for protection of classified material. **Note:** for emergency plan requirements pertaining to special access program (SAP), sensitive compartmented information (SCI) and/or communications security (COMSEC), contact your local program security officer, special security officer or COMSEC custodian.

b. Although the importance of protecting collateral material cannot be discounted, it must be accomplished in such a way as to minimize the risk of loss of life or injury to employees.

3. Actions

a. If there is no imminent danger to employees:

(1) Thoroughly check workspaces for unsecured collateral material prior to departure.

(2) Secure collateral material in authorized containers before evacuation.

(a) If authorized storage is not immediately available, attempt to carry collateral material from the area, seeking assistance from other cleared personnel, as needed.

(b) Should circumstances require that some collateral material be left unattended, immediately report this fact to the local security office.

(c) The holder will notify the senior government official, or incident commander at the central evacuation point that they are holding classified material or that classified materials has been left unsecured in the work area. The holder will provide the location, type of classified (i.e., media, documents, etc.) and the approximate amount. Protect the classified material until the emergency is terminated or take action to secure it in an approved security container. Individual is responsible for returning the classified information to the proper security container unless otherwise directed by the commander or the security manager. Under no circumstances will the classified material be transported to the holder's private living quarters.

(3) Upon cancellation of the emergency situation and when given the authorization to do so, employees will return to the work area and inventory any unsecured collateral material, reporting the results of this action to the security office. As appropriate, employees will also check security containers, secure rooms, and vaults for evidence of forced entry.

b. If there is imminent danger to employees:

(1) Evacuate immediately, leaving collateral material in place. Under no circumstances should employees endanger themselves attempting to secure or remove classified information from workspaces.

(2) When possible, report the existence of unattended collateral material to the area supervisor who will then, as conditions allow, either arrange for monitoring of the area perimeter or contact the security office to report the situation.

c. Should destruction of collateral material be warranted (e.g., enemy/terrorist attack):

(1) When possible, collateral material should be destroyed using equipment previously authorized for classified destruction (e.g., approved shredders and degaussers).

(2) When such equipment is not available, or circumstances otherwise dictate, collateral material may be destroyed by any means that will ensure positive destruction of the material (e.g., burned).

(3) As possible, document the destruction of all accountable collateral material by noting, at a minimum, the accountability number (e.g., barcode or serial number).

(4) Report the overall destruction totals to local security office.

d. Should circumstances preclude the protection or destruction of all collateral material, then appropriate prioritization should occur based on the classification level of the material. Consequently, the protection/destruction of top secret material must take precedence over secret material, and so on.

4. Responsibilities. Management, at all levels, will ensure that these procedures are posted to allow for easy access by personnel responsible for safeguarding collateral material.

Office Point of Contact: _____ **Phone:** _____

Security Point of Contact: _____ **Phone:** _____

ENCLOSURE 3

STORAGE AND DESTRUCTION

1
2
3
4
5
6
7 1. GENERAL REQUIREMENTS
8

9 a. Classified information shall be secured under conditions adequate to deter and detect access
10 by unauthorized persons. The requirements specified in this Volume represent acceptable security
11 standards. DoDD 5210.56 (Reference (ai)) specifies DoD policy concerning the use of force for the
12 protection of classified information. Do not store weapons or items such as funds, jewels, precious
13 metals, or drugs in the same container used to safeguard classified information. Holdings of
14 classified material should be reduced to the minimum required to accomplish the mission.
15

16 b. GSA establishes and publishes minimum standards, specifications, and supply schedules for
17 containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for
18 storing and protecting classified information. DoDI 3224.03 (Reference (aj)) describes
19 requirements for acquiring physical security equipment for use within the Department of Defense.
20

21 c. The DNI establishes security requirements for sensitive compartmented information
22 facilities (SCIFs). These are issued by Reference (i) within the DoD.
23

24 d. The DoD Lock Program is designated as the DoD technical authority for locking and
25 storage systems used for the protection of classified information. For technical support, call the
26 DoD Lock Program Technical Support Hotline at 1-800-290-7607 or DSN 551-1212 or review the
27 website at <https://locks.navfac.navy.mil>, for more information.
28

29 e. DoDI 5200.48 specifies storage and destruction requirements for controlled unclassified
30 information.
31

32 **f. (Added)(DAF) When foreign military sales (FMS) requirements exist, the responsible**
33 **DAF program office will validate that the processing, storing and destruction of classified**
34 **information is commensurate to the level of protection as provided by the U.S. government,**
35 **consistent with DoD 5105.38-M, *Security Assistance Management Manual (SAMM)*. (T-0).**
36
37

38 2. LOCK SPECIFICATIONS. Except as provided elsewhere in this Volume, combination locks
39 on vault doors, secure rooms, and security containers protecting classified information shall
40 conform to Federal Specification FF-L-2740 (hereafter referred to as “FF-L-2740”) (Reference
41 (aj)).
42

43
44 3. STORAGE OF CLASSIFIED INFORMATION BY LEVEL OF CLASSIFICATION. Store
45 classified information not under the personal control and observation of an authorized person, in a
46 locked security container, vault, room, or area, as specified in this section.
47

48 a. Top Secret. Top Secret information shall be stored:
49

50 (1) In a GSA-approved security container with one of the following supplementary
51 controls;

52
53 (a) An employee cleared to at least the Secret level shall inspect the security container
54 once every 2 hours.

55
56 (b) The location that houses the security container is protected by an intrusion
57 detection system (IDS) meeting the requirements of the Appendix to this enclosure with personnel
58 responding to the alarm arriving within 15 minutes of the alarm annunciation.

59
60 (2) In a GSA-approved security container equipped with a lock meeting FF-L-2740,
61 provided the container is located within an area that has been determined to have security-in-depth
62 (see Glossary for definition);

63
64 (3) In an open storage area (also called a secure room) constructed according to the
65 Appendix to this enclosure and equipped with an IDS with the personnel responding to an alarm
66 within 15 minutes of the alarm annunciation if the area has been determined to have security-in-
67 depth, or within 5 minutes of alarm annunciation if it has not;

68
69 (4) In a vault, or GSA-approved modular vault, meeting the requirements of Federal
70 Standard (FED-STD) 832 (Reference (al)) as specified in the Appendix to this enclosure; or

71
72 (5) Under field conditions during military operations, using such storage devices or
73 security control measures as a military commander deems adequate to prevent unauthorized access.
74 Military commanders should employ risk management methodologies when determining
75 appropriate safeguards.

76
77 b. Secret. Secret information shall be stored by one of the following methods:

78
79 (1) In the same manner as prescribed for top secret information;

80
81 (2) In a GSA-approved security container or vault built to FED-STD 832 specifications,
82 without supplementary controls;

83
84 (3) In an open storage area meeting the requirements of the Appendix to this enclosure,
85 provided the senior agency official determines in writing that security-in-depth exists, and one of
86 the following supplemental controls is utilized.

87
88 (a) An employee cleared to at least the Secret level shall inspect the open storage area
89 once every 4 hours.

90
91 (b) An IDS meeting the requirements of the Appendix to this enclosure with the
92 personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

93
94 (4) In a secure room that was approved for the storage of Secret information by the DoD
95 Component prior to October 1, 1995, provided the DoD Component reassesses the requirement for
96 the secure room and makes plans to bring the room up to the standards of subparagraphs 3.b.(1)
97 through 3.b.(3) of this section by October 1, 2013 and provided the area has been determined to
98 have security-in-depth.

99

100 (5) ***(Added)(DAF) The servicing IP office must ensure all open storage rooms**
101 **approved for storage of classified information meet appropriate safeguarding standards. (T-**
102 **1). If rooms do not meet standards, or where the original justification for open storage is no**
103 **longer valid, the rooms must be decertified. (T-0). Upon decertification, commander or**
104 **director has two options: 1) keep the room/area under constant 24/7 surveillance; or, 2) use**
105 **other approved storage means. (T-1).**

106

107 c. Confidential. Confidential information shall be stored in the same manner as prescribed for
108 top secret or secret information except that supplemental controls are not required.

109

110

111 4. RISK ASSESSMENT. When considering the storage alternatives specified in section 3, a risk
112 assessment shall be performed to facilitate a security-in-depth determination and to aid
113 identification and selection of supplemental controls that may need to be implemented. The
114 analysis should, at a minimum, consider local threats, both known and anticipated, and
115 vulnerabilities; the existing security environment and controls; the ease of access to containers or
116 other areas where classified data is stored; the criticality, sensitivity, and value of the information
117 stored; and cost verses benefits of potential countermeasures. The risk assessment shall be used to
118 determine whether installation of an IDS is warranted or whether other supplemental controls are
119 sufficient.

120

121 a. **(Added)(DAF) The DAF SAO has delegated the authority to make security-in-depth**
122 **determinations to the MAJCOM/FLDCOM SPE and commanders or directors under their**
123 **control or authority, when determining supplemental controls.**

124

125 b. ***(Added)(DAF) The cognizant commander or director will conduct a risk assessment**
126 **for each GSA-approved security container storing classified information located outside of an**
127 **open storage area (secure room) and all open storage areas approved to store top secret**
128 **information. (T-1). Risk assessments and security-in-depth determinations must be**
129 **documented. (T-1).**

130

131

132 5. U.S. CLASSIFIED INFORMATION LOCATED IN FOREIGN COUNTRIES. Except for
133 classified information that has been authorized for release to a foreign government or international
134 organization in accordance with Reference (z), and is under that government's or organization's
135 security control, U.S. classified material may be retained and stored in a foreign country only when
136 necessary to satisfy specific U.S. Government requirements. The Heads of the DoD Components
137 shall prescribe requirements for protecting this information, paying particular attention to ensuring
138 proper enforcement of controls on release of U.S. classified information to foreign entities.
139 Compliance with the provisions of this enclosure is required. U.S. classified material in foreign
140 countries shall be stored at a:

141

142 a. U.S. military installation, or a location where the U.S. enjoys extraterritorial status, such as
143 an embassy or consulate.

144

145 b. U.S. Government activity located in a building used exclusively by U.S. Government
146 tenants, provided the building is under continuous (i.e., 24/7) control by U.S. Government
147 personnel.

148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196

c. U.S. Government activity located in a building not used exclusively by U.S. Government tenants which is under host government control, provided that the classified material is stored in GSA-approved security containers which are further secured in a locked room or area to which only U.S. personnel have access and the room or area is under continuous (i.e., 24/7) control by U.S. Government personnel.

d. U.S. Government activity located in a building not used exclusively by U.S. Government tenants nor under host-government control, provided the classified material is stored in GSA-approved security containers and is placed under continuous (i.e., 24/7) control by U.S. Government personnel.

6. SPECIALIZED STORAGE

a. Military Platforms

(1) The Heads of the DoD Components shall, consistent with this Volume, delineate the appropriate security measures required to protect classified information stored in security containers on military platforms (e.g., aircraft, militarized or tactical vehicle) and for classified munitions items.

(2) GSA-approved field safes and special size one- and two-drawer security containers approved by the GSA may be used for storage of classified information in the field and in military platforms. These containers shall use locks conforming to FF-L-2740 or Federal Specification FF-L-2937 (Reference (am)), as required by Federal Specification AA-F-358 (Reference (an)). Special size containers shall be securely fastened to the platform; field safes shall be under sufficient control and surveillance when in use to prevent unauthorized access or loss.

(3) *(Added)(DAF) Aircraft

(a) (Added)(DAF) All personnel with access to DAF aircraft must have security clearance eligibility and access at the appropriate level as well as a valid need-to-know prior to performing maintenance on aircraft parts or components that contain classified information. (T-1). Passengers and other un-cleared personnel will be properly escorted, at all times, to prevent unauthorized access to classified material aboard. (T-0).

1. (Added)(DAF) Installation, maintenance, depot, acquisition program manager, and aircraft commanders are responsible for the security of aircraft while under their control and must consult the servicing IP office to determine the appropriate safeguarding standards for classified material and components aboard aircraft at their home station. (T-1).

2. (Added)(DAF) Aircraft commanders must consult with their servicing installation IP office (or program security officer (PSO) and special security officer (SSO), if applicable), during mission planning, to determine the appropriate safeguarding standards for classified material and components aboard aircraft, at civilian airports within the U.S., non-USG military installations outside the U.S., and civilian airports outside the U.S. (T-1). Aircraft commanders are responsible for ensuring protection of classified material and

197 components aboard their aircraft while away from their home station. (T-1). Aircraft
198 commanders may make certain risk management precautions when diverted, experience an
199 in-flight emergency, or are required to make an unplanned landing to protect classified
200 information material aboard their aircraft. COMSEC program managers must be consulted
201 for allowable risks associated with this program (T-1).
202

203 (b) (Added)(DAF) Protection level (PL) 1, 2, 3, or 4 aircraft storing classified
204 material or components must be parked inside a temporary or permanent DAF
205 restricted/controlled area, or an equivalent sister-service area, while on a DoD installation
206 and/or facility. (T-1). Consult the servicing IP office (or PSO and SSO, if applicable) for
207 additional security measures.
208

209 (c) *(Added)(DAF) At USG installations or facilities, ensure PL 1 – 4 aircraft are
210 left under the personal control and observation of an authorized USG person, with the proper
211 security clearance eligibility and access. (T-1). If an authorized USG person is not available,
212 coordinate with the host USG military police or security forces and the servicing IP office (or
213 PSO and SSO, if applicable) to determine amenable safeguarding accommodations. (T-1).
214 Designated personnel shall:
215

216 1. (Added)(DAF) Zeroize keyed COMSEC equipment in accordance with
217 DAFMAN 17-1302-O, *Communications Security (COMSEC) Operations*. (T-0).
218

219 2. (Added)(DAF) Secure removable classified components and material that
220 are not attached or secured to the aircraft in an approved storage container. (T-1). If the
221 aircraft is not equipped with an approved storage container or the items are too large, consult
222 with the servicing IP office (PSO or SSO) to secure proper storage. (T-1). Classified
223 components attached to the aircraft do not have to be removed, provided visual access
224 doesn't present security concerns.
225

226 3. (Added)(DAF) Secure all egress doors from the inside if classified
227 components and material must remain with the aircraft. (T-1). If this is not possible, secure
228 the egress points from the outside using a GSA-approved combination padlock that meets
229 *Federal Specifications FF-P-110J, Padlock, Changeable Combination (Resistant to Opening by*
230 *Manipulation and Surreptitious Attack)*, (reference (ao)), as amended. (T-0).
231

232 4. (Added)(DAF) If the aircraft cannot be locked or is not equipped with an
233 authorized storage container, place the removable classified material in an approved security
234 container, in a facility authorized for the storage. (T-1).
235

236 (d) (Added)(DAF) At civilian airports within the continental United States
237 (CONUS), non-USG military installations outside [the] continental United States (OCONUS),
238 and civilian airports OCONUS:
239

240 1. (Added)(DAF) Place removable classified material in a security container
241 aboard the aircraft, and secure the aircraft. (T-1). The aircrew must conduct aircraft and
242 security container checks every 4 hours. (T-1). This check must be conducted within 1 hour
243 after official aircrew rest, if no other USG personnel are available. (T-1).
244

245 2. (Added)(DAF) If the aircraft does not have a security container and no USG

246 facility is available, the aircraft must be kept under constant surveillance by cleared USG
247 personnel. (T-1).
248

249 (e) (Added)(DAF) Commanders must take prudent risk management precautions
250 when diverted or experience in-flight emergencies to protect classified information to include
251 COMSEC material aboard their aircraft. (T-1).
252

253 (4) (Added)(DAF) The installation commander, in collaboration with the servicing IP
254 office, may authorize the use of a non-GSA approved security container aboard military
255 platforms to store classified material, under unique mission requirements. The approval
256 must be documented, in writing, and contain the explanation of the special circumstances
257 warranting deviation from standards, as well as a description of the administrative
258 procedures for the control and accounting of locks. (T-1). Place all removable classified
259 material (e.g., paper documents, hard drives, and magnetic media) in a storage container
260 secured with a GSA-approved three position dial-type lock. (T-1). The storage container
261 must be a seamless metal (or similar construction) box or one with welded seams and a
262 lockable door in order to prevent, deter and detect surreptitious entry. (T-1). The container
263 must be secured to the aircraft, and the hinges must be either internally mounted or welded.
264 (T-1). Under these circumstances, containers installed for storage of weapons may also be
265 used to store classified material.
266

267 (a) (Added)(DAF) In unique circumstances, the installation commander may
268 authorize, in coordination with the servicing IP office, the use of key operated locks in place
269 of a three positioned dial-type lock.
270

271 (b) A description of administrative procedures for the control and accountability
272 of keys and locks must be maintained. (T-1). Keys must be safeguarded commensurate to the
273 level of information being protected. (T-1). Keys and locks will be audited semi-annually;
274 document the audit using AF Form 2427, *Lock and Key Control Register*. (T-1).
275

276 b. IT Equipment. GSA-approved information processing system cabinets are available for
277 protection of operational IT equipment. The cabinets can be used for storage of network equipment
278 (such as routers, switches, and crypto devices), servers, power control units, and laptops and can be
279 configured for rack mounting with interior fans for heat management and cable connections for
280 exterior data transmission and power.
281

282 c. Map and Plan File Cabinets. GSA-approved map and plan file cabinets are available for
283 storing odd-sized items such as computer media, maps, charts, and classified equipment.
284

285 d. Modular Vaults. GSA-approved modular vaults meeting Federal Specification AA-V- 2737
286 (Reference (ao)) may be used to store classified information as an alternative to vault requirements
287 described in the Appendix to this enclosure.
288

289 e. Bulky Material. Storage areas for bulky material containing Secret or Confidential
290 information may have access openings (e.g., roof hatches, vents) secured by GSA-approved
291 changeable combination padlocks meeting Federal Specification FF-P-110 (Reference (ao)). Other
292 security measures are required, in accordance with paragraphs 3.b. and 3.c. of this enclosure.
293

294 (1) When special circumstances exist, the Heads of the DoD Components may authorize

295 the use of key operated locks for storing bulky material containing secret and confidential
296 information. The authorization shall be documented with an explanation of the special
297 circumstances that warrant deviation from other established standards. Whenever using such locks,
298 administrative procedures for the control and accounting of keys and locks shall be established.
299 The level of protection provided to such keys shall be equivalent to that afforded the classified
300 information the padlock protects.

301
302 (2) Section 1386 of title 18, United States Code (U.S.C.) (Reference (aq)), makes
303 unauthorized possession of keys, key-blanks, keyways, or locks that any part of the Department of
304 Defense adopts for protecting conventional arms, ammunition, or explosives, special weapons, and
305 classified equipment, a criminal offense punishable by fine or imprisonment for up to
306 10 years, or both.

307
308 **(3) *(Added)(DAF) If authorized, codify key and lock control procedures in the**
309 **organization's security instruction or plan and document key and lock accountability on the**
310 **AF Form 2427. (T-1). Unless determined otherwise, the commander or director will**
311 **inventory keys and locks annually, during compliance self-inspections. (T-1).**
312

313
314 7. PROCURING NEW STORAGE EQUIPMENT. New security storage equipment shall be
315 procured from those items listed on the GSA Federal Supply Schedule. When GSA-approved
316 security containers or vault doors with locks meeting FF-L-2740 are placed in service or when
317 existing mechanical locks are replaced with locks meeting FF-L-2740, the custodian or security
318 manager shall record the lock serial number on an SF 700, "Security Container Information." For
319 procurement or technical support, call the DoD Lock Program as specified in paragraph 1.d of this
320 enclosure.

321
322
323 8. SECURITY CONTAINER LABELS. GSA-approved security containers must have a label
324 stating "General Services Administration Approved Security Container," affixed to the front of the
325 container, usually on the control or the top drawer.

326
327 a. If the label is missing or if the container's integrity is in question, the container shall be
328 inspected by a GSA-certified inspector. Information on obtaining inspections and recertification of
329 containers can be found on the DoD Lock Program Website (<https://locks.navfac.navy.mil>) or by
330 calling the DoD Lock Program at (800) 290-7607 or DSN 551-1212.

331
332 b. When the container is being sent to the Defense Reutilization and Marketing Office, the
333 GSA label shall be removed.

334
335
336 9. EXTERNAL MARKINGS ON CONTAINERS
337

338 a. There shall be no external mark revealing the level of classified information authorized to
339 be or actually stored in a given container or vault, or indicating the priority assigned to the
340 container for emergency evacuation and destruction. This does not preclude placing a mark or
341 symbol (e.g., a bar code) on the container for other purposes (e.g., identification and/or inventory
342 purposes) or from applying decals or stickers the DNI requires for containers and equipment used
343 to store or process intelligence information. If a GSA container or vault door recertification is

344 required, such labels and markings must be removed, but may be reapplied as needed after
345 recertification.

346

347 **b. *(Added)(DAF) In areas where natural disasters may result in the destruction of**
348 **facilities; or, where strong winds or flooding may displace security containers, the**
349 **commander or director will use some type of inventory control marking to facilitate recovery**
350 **of security containers, once the installation is cleared to commence operations. (T-1).**
351 **Security container recovery should be part of the annual exercise of emergency plans under**
352 **Enclosure 2, paragraph 10.**

353

354

355 10. SECURITY CONTAINER INFORMATION. Maintain a record for each container, or vault or
356 secure room door, used for storing classified information. SF 700 with all information blocks
357 completed, shall be used for this purpose. Update the form each time the security container
358 combination is changed.

359

360 a. Part 1 of SF 700 is not classified, but contains personally identifiable information (PII) that
361 shall be protected by sealing Part 1 in an opaque envelope (not provided as part of the SF 700)
362 conspicuously marked "Security Container Information" and stored in accordance with SF 700
363 instructions. If the information must be accessed during non-duty hours and a new opaque
364 envelope is not available to replace the opened one, the original envelope should be temporarily
365 resealed, to the extent possible, until Part 1 can be placed in a new envelope the next working day.

366

367 b. Part 2 of SF 700, when completed, is classified at the highest level of classification
368 authorized for storage in the security container. It shall be sealed and stored in accordance with SF
369 700 instructions. The classification authority block shall state "Derived From: 32 CFR
370 2001.80(d)(3)," with declassification date being, "upon change of combination."

371

372 **c. *(Added)(DAF) The security container, secure room or vault door custodian is**
373 **responsible for completing required inspections, using appendix 2, to this enclosure, and**
374 **performing combination changes. (T-1). Custodians are encouraged to use the Center for**
375 **Development of Security Excellence resources to be proficient in their responsibilities.**
376 **Consult with the servicing IP office for guidance and when maintenance and/or repairs are**
377 **outside their skills and abilities. Maintenance and repairs will be documented on the**
378 **Optional Form 89, *Maintenance Record for Security Containers/ Vault Doors*. (T-1). (Note:**
379 **Do not record combination changes on the Optional Form 89).**

380

381

382 11. COMBINATIONS TO CONTAINERS, VAULTS AND SECURE ROOMS

383

384 a. Protecting and Storing Combinations. In accordance with section 2001.45(a)(1) of
385 Reference (f), the combination shall be classified at the same level as the highest classification of
386 the material authorized for storage in the container.

387

388 (1) Use SF 700 Part 2, as specified in section 10 of this enclosure, to record the
389 combination and other required data.

390

391 (2) If another record of the combination is made, the record shall be marked as required by
392 Volume 2 of this Manual.

393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441

(3) Only a minimum number of authorized persons shall have knowledge of combinations to authorized storage containers, including vaults and secure rooms.

(4) Security containers, vaults, secure rooms and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

(5) A record of the names of persons having knowledge of the combination shall be maintained.

b. Changing Combinations. Only individuals with the responsibility and an appropriate security clearance shall change combinations to security containers, vaults and secure rooms used for storing classified information. Combinations shall be changed:

(1) When the container, vault, or secure room door is placed in service.

(2) Whenever an individual knowing the combination to the container or vault door no longer requires access, unless other sufficient controls exist to prevent that individual's access to the lock.

(3) When compromise of the combination is suspected.

(4) When the container, vault, or secure room door is taken out of service or is no longer used to store classified information, at which time built-in combination locks shall be reset to the standard combination 50-25-50, and combination padlocks shall be reset to the standard combination 10-20-30.

12. ENTRANCES TO OPEN STORAGE AREAS FOR CLASSIFIED INFORMATION

a. When areas storing classified information are occupied by authorized individual(s), the entrances shall either be:

(1) Under visual control at all times to detect entry by unauthorized persons; or

(2) Equipped with an automated entry control system to limit access (see section 3 of the Appendix to this enclosure).

b. Secure rooms or other areas storing classified information shall be secured when the area is not occupied by authorized individual(s) or under continual visual control.

c. The Appendix to this enclosure provides standards for access control devices. Electrically actuated locks (e.g., magnetic strip card locks) do not, by themselves, meet the required standards for protecting classified information and shall not be used as a substitute for the locks prescribed in section 2 of this enclosure.

13. INSPECTION OF STORAGE CONTAINERS PRIOR TO REMOVAL, REPAIR, ETC.

442 Cleared personnel shall inspect storage containers that may have been used to store classified
443 information before removing them from protected areas or allowing unauthorized persons access to
444 them to ensure no classified material remains within.

445

446

447 14. NEUTRALIZATION AND REPAIR PROCEDURES. The procedures described in FED-
448 STD 809 (Reference (ar)) shall be followed for neutralization and repair of security containers and
449 vault doors. Reference (ar) can be found on the DoD Lock Program Website,
450 <https://locks.navfac.navy.mil>.

451

452 a. Neutralization and repair of a security container or door to a vault approved for storage of
453 classified information shall be accomplished only by appropriately cleared or continuously escorted
454 personnel specifically trained in the methods specified by Reference (ar).

455

456 b. Neutralization or repair by, or using, methods and procedures other than described in
457 Reference (ar) is considered a violation of the security container's or vault door's security integrity
458 and the GSA label shall be removed. Thereafter, the containers or doors may not be used to protect
459 classified information.

460

461

462 15. STORAGE OF FGI. To the extent practical, FGI shall be stored separately from other
463 information to facilitate its control. To avoid additional costs, separate storage may be
464 accomplished by methods such as using separate drawers in the same container as other
465 information or, for small amounts, the use of separate file folders in the same drawer.

466

467

468 16. RETENTION OF CLASSIFIED INFORMATION. Classified documents and other material
469 shall be retained within DoD organizations only if they are required for effective and efficient
470 operation of the organization or if law or regulation requires their retention. Documents no longer
471 required for operational purposes shall be disposed of according to the provisions of chapter 33 of
472 Reference (t) and appropriate implementing directives and records schedules, and in accordance
473 with sections 17 and 18 of this enclosure.

474

475

476 17. DESTRUCTION OF CLASSIFIED INFORMATION. Classified documents and material
477 identified for destruction shall be destroyed completely, to prevent anyone from reconstructing the
478 classified information, according to procedures and methods the DoD Component Head prescribes.
479 Methods and equipment used to routinely destroy classified information include burning, crosscut
480 shredding, wet pulping, mutilation, chemical decomposition or pulverizing. Methods used for
481 clearing, sanitization or destruction of classified IT equipment and media include overwriting,
482 degaussing, sanding, and physical destruction of components or media.

483

484 a. Documents and other material identified for destruction shall continue to be protected as
485 appropriate for their classification until actually destroyed.

486

487 b. Each activity with classified holdings shall establish at least 1 day each year when specific
488 attention and effort is focused on disposing of unneeded classified material ("clean-out day").

489

490 c. Guidance on standards, processes, and procedures for the destruction of COMSEC and other

491 classified material can be found in Reference (r). NATO material shall be destroyed in accordance
 492 with Reference (ac). FGI shall be destroyed in the same manner as U.S. classified information of
 493 the equivalent level, except where otherwise required by international treaty or agreement. Also
 494 see Enclosure 2, subparagraphs 17.b.(7)(a) through (d) for guidance on recording FGI destruction.
 495

496 d. Effective January 1, 2011, only equipment listed on an evaluated products list (EPL) issued
 497 by NSA may be used to destroy classified information using any method covered by an EPL. EPLs
 498 currently exist for paper shredders, punched tape destruction devices, optical media destruction
 499 devices (for compact discs (CDs) and digital video discs (DVDs)), degaussers (for magnetic media
 500 sanitization), and disintegrators (for paper and punched tape material). The EPLs may be obtained
 501 by calling (410) 854-6358 or at
 502 http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml.
 503

504 (1) Equipment approved for use prior to January 1, 2011, and not found on the appropriate
 505 EPL may be used for destruction of classified information until December 31, 2016.
 506

507 (2) Unless determined otherwise by NSA, whenever an EPL is revised, equipment
 508 removed from the EPL may be utilized for destruction of classified information for up to 6 years
 509 from the date of its removal from the EPL.
 510

511 (3) In all cases, if any such previously approved equipment needs to be replaced or
 512 otherwise requires a rebuild or replacement of a critical assembly (e.g., shredder blade assembly),
 513 the unit must be replaced with one listed on the appropriate EPL.
 514

515 (4) Classified IT storage media (e.g., hard drives) cannot be declassified by overwriting.
 516 Sanitization (which may destroy the usefulness of the media) or physical destruction is required for
 517 disposal. See also section 6 of Enclosure 7 of this Volume.
 518

519
 520 18. TECHNICAL GUIDANCE ON DESTRUCTION METHODS. Contact the National Security
 521 Agency/Central Security Service (NSA/CSS) System and Network Analysis Center at (410) 854-
 522 6358 or via e-mail at SNAC@radium.ncsc.mil, to obtain technical guidance concerning appropriate
 523 methods, equipment, and standards for destroying classified electronic media, IT equipment,
 524 electronic components, and other similar or associated materials.
 525

526 a. Crosscut Shredders. Only crosscut shredders listed on the “NSA/CSS Evaluated Products
 527 List for High Security Crosscut Paper Shredders” (Reference (as)) may be used to destroy classified
 528 material by shredding.
 529

530 (1) The EPL is updated on an as-needed basis as new models are successfully evaluated.
 531 Users are encouraged to contact shredders manufacturers and/or distributors for assistance in
 532 selecting unit(s) best suited to their requirements. Vendors and/or distributors can provide
 533 guidance on whether a specific model not listed meets the specifications in Reference (as) (e.g., for
 534 shred size) and, as applicable, a copy of the NSA/CSS letter confirming that the model will be
 535 included on the EPL at its next update.
 536

537 (2) Crosscut shredders currently in use and not on the EPL that were at the time of
 538 acquisition on a NSA/CSS evaluated approved products list as being capable of maintaining a shred
 539 size of 1/2 inch by 1/32 inch (variance of 1/64 inch) may be used until December 31, 2016 in

540 accordance with paragraph 17.d of this enclosure, EXCEPT for destruction of COMSEC materials.
541 However, any such crosscut shredders requiring replacement of the unit and/or rebuild of the
542 shredder blades assembly MUST BE REPLACED by a crosscut shredder on the latest NSA/CSS
543 EPL. When COMSEC material is destroyed by shredding, ONLY crosscut shredders listed in
544 Reference (as) at the time of acquisition shall be used.
545

546 (a) Pending replacement, the Heads of DoD Components shall ensure that procedures
547 are in place to manage the risk posed by crosscut shredders not on the approved NSA/CSS list. At a
548 minimum, the volume and content of each activity's classified material destruction flow shall be
549 assessed and a process established to optimize the use of high security crosscut paper shredders
550 (i.e., with top secret collateral material being the highest collateral priority) to take full advantage
551 of the added security value of those shredders.
552

553 (b) The bag of shred must be "stirred" to ensure that the content is mixed up.
554

555 (c) Shredding of unclassified material along with the classified material is encouraged.
556

557 b. Pulverizers and Disintegrators. Pulverizers and disintegrators must have a 3/32 inch or
558 smaller security screen. Consult the "NSA/CSS Evaluated Products List for High Security
559 Disintegrators," (Reference (at)) for additional details and guidance.
560

561 c. Pulping. Pulping (wet process) devices with a 1/4 inch or smaller security screen may be
562 used to destroy classified water-soluble material.
563

564 19. DESTRUCTION PROCEDURES 565

566
567 a. The Heads of the DoD Component shall establish procedures to ensure that all classified
568 information intended for destruction is destroyed by authorized means and appropriately cleared
569 personnel.
570

571 b. Classified information that cannot be destroyed shall be reevaluated and, when appropriate,
572 downgraded, declassified, or retired to a designated record center.
573

574 c. Classified information shall be controlled in a manner designed to minimize the possibility
575 of unauthorized removal and/or access. A burn bag may be used to store classified information
576 awaiting destruction at a central destruction facility. Seal and safeguard each burn bag per this
577 Volume until actually destroyed.
578

579 d. Records of destruction are not required, except as noted in paragraph 17.c of this enclosure
580 and, for destruction of classified FGI, in Enclosure 2, subparagraphs 17.b.(7)(a) through (d).
581

582 Appendix

583 Physical Security Standards

584 ***(Added)(DAF) Security Container, Vault Door and Secure Room Visual Inspection**
585 **Checklist**

586 APPENDIX 1 TO ENCLOSURE 3

587 PHYSICAL SECURITY STANDARDS

588
589
590
591 1. VAULT AND SECURE ROOM CONSTRUCTION STANDARDS

592
593 a. Vaults. Vaults shall be constructed to meet Reference (al) as follows:

594
595 (1) Class A (concrete poured-in-place).

596
597 (2) Class B (GSA-approved modular vault meeting Reference (ao) specifications).

598
599 (3) Class C (steel-lined vault) is NOT authorized for protection of classified
600 information.

601
602 b. Open Storage Area (Secure Room). This section provides the minimum construction
603 standards for open storage areas.

604
605 (1) Walls, Floor, and Roof. Walls, floor, and roof shall be of permanent construction
606 materials (i.e., plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other
607 materials) offering resistance to and evidence of unauthorized entry into the area. Walls shall be
608 extended from the true floor to the true ceiling and attached with permanent construction
609 materials, mesh, or 18 gauge expanded steel screen.

610
611 (2) Ceiling. The ceiling shall be constructed of plaster, gypsum, wallboard material,
612 hardware or any other acceptable material.

613
614 (3) Doors. Access doors shall be substantially constructed of wood or metal. For out-
615 swing doors, hinge-side protection shall be provided by making hinge pins non-removable (e.g.,
616 spot welding) or by using hinges with interlocking leaves that prevent removal. Doors shall be
617 equipped with a GSA-approved combination lock meeting FF-L-2740. Doors other than those
618 secured with locks meeting FF-L-2740 shall be secured from the inside with deadbolt emergency
619 egress hardware, a deadbolt, or a rigid wood or metal bar that extends across the width of the
620 door.

621
622 (4) Windows

623
624 (a) Windows that are less than 18 feet above the ground measured from the bottom
625 of the window, or are easily accessible by means of objects located directly beneath the
626 windows, shall be constructed from or covered with materials that will provide protection from
627 forced entry. The protection provided to the windows need be no stronger than the strength of
628 the contiguous walls. Secure rooms which are located within a controlled compound or
629 equivalent may eliminate the requirement for forced entry protection if the windows are made
630 inoperable either by permanently sealing them or equipping them on the inside with a locking
631 mechanism and they are covered by an IDS (either independently or by motion detection sensors

632 within the area).

633

634 (b) Windows, which might reasonably afford visual observation of classified
635 activities within the facility shall be made opaque or equipped with blinds, drapes, or other
636 coverings.

637

638 (5) Utility Openings. Utility openings such as ducts and vents shall be smaller than
639 man- passable (96 square inches). An opening larger than 96 square inches (and over 6 inches in
640 its smallest dimension) that enters or passes through an open storage area shall be hardened in
641 accordance with Military Handbook 1013/1A (Reference (au)).

642

643 **c. *(Added)(DAF) When classified information is processed in a space that does not**
644 **meet open storage requirements, it must be evaluated by the servicing IP and cybersecurity**
645 **offices, prior to installation of the classified information system. (T-1).**

646

647

648 2. IDS STANDARDS

649

650 a. IDS Purpose. An IDS shall detect an unauthorized penetration into the secured area. An
651 IDS shall be installed when results of a documented risk assessment determine its use as a
652 supplemental control is warranted, in accordance with Enclosure 3, sections 3 and 4 of this
653 Volume, and use is approved by the activity head. When used, all areas that reasonably afford
654 access to the security container or areas where classified data is stored shall be protected by IDS
655 unless continually occupied. An IDS complements other physical security measures and consists
656 of:

657

658 (1) Intrusion detection equipment (IDE)

659

660 (2) Security forces

661

662 (3) Operating procedures

663

664 **(4) *(Added)(DAF) When IDS is used as a supplemental control:**

665

666 **(a) (Added)(DAF) If the IDS malfunctions and the risk assessment has**
667 **determined 2 hour (top secret) or 4 hour (secret) checks are sufficient, then the owning**
668 **activity's commander or director shall conduct and document these checks. (T-1).**

669

670 **(b) If the IDS malfunctions and the risk assessment determined that the IDS**
671 **was a required supplemental control that could not be augmented, then the secure room**
672 **must be kept under 24/7 surveillance, until the IDS is repaired. (T-1).**

673

674 b. System Functions

675

676 (1) IDS components operate as a system with four distinct phases:

677

678 (a) Detection

679

680 (b) Communications

681

682 (c) Assessment

683

684 (d) Response

685

686 (2) These elements are equally important, and none can be eliminated if an IDS is to
687 provide an acceptable degree of protection.

688

689 (a) Detection. During the detection phase, a detector or sensor senses and reacts to
690 the stimuli it is designed to detect. The sensor alarm condition is then transmitted over cabling
691 located within the protected area to the premise control unit (PCU). The PCU may service many
692 sensors. The PCU and the sensors it serves comprise a zone at the monitor station (i.e., an
693 alarmed zone).

694

695 (b) Communications. The PCU receives signals from all sensors in a protected area
696 and incorporates these signals into a communication scheme. An additional signal is added to
697 the communication for supervision to prevent compromise of the communication scheme (i.e.,
698 tampering or injection of false information by an intruder). The supervised signal is sent by the
699 PCU through the transmission link to the monitor station. Inside the monitor station either a
700 dedicated panel or central processor monitors information from the PCU signals. When an alarm
701 occurs, an annunciator generates an audible and visible alert to security personnel. Alarms result
702 normally from intrusion, tampering, component failure, or system power failure.

703

704 (c) Assessment. The assessment period is the first phase that requires human
705 interaction. When alarm conditions occur, the operator assesses the situation and dispatches the
706 response force.

707

708 (d) Response. The response phase begins as soon as the operator assesses an alarm
709 condition. A response force shall immediately respond to all alarms. The response phase shall
710 also determine the precise nature of the alarm and take all measures necessary to safeguard the
711 secure area.

712

713 c. Acceptability of Equipment. All IDE must be Underwriters Laboratories (UL)-listed (or
714 equivalent) and approved by the DoD Component. Government installed, maintained, or
715 furnished systems are acceptable.

716

717 d. Transmission and Annunciation

718

719 (1) Transmission Line Security. When the transmission line leaves the facility and
720 traverses an uncontrolled area, Class I or Class II line supervision shall be used.

721

722 (a) Class I. Class I security is achieved through the use of Data Encryption
723 Standard or an algorithm based on the cipher feedback or cipher block chaining mode of

724 encryption. Certification by the National Institutes of Standards and Technology or another
725 independent testing laboratory is required.

726

727 (b) Class II. Class II line supervision refers to systems in which the transmission is
728 based on pseudo-random generated tones or digital encoding using an interrogation and response
729 scheme throughout the entire communication, or UL Class AA line supervision. The signal shall
730 not repeat itself within a minimum 6-month period. Class II security shall be impervious to
731 compromise using resistance, voltage, current, or signal substitution techniques.

732

733 (2) Internal Cabling. The cabling between the sensors and the PCU shall be dedicated
734 to IDE and shall comply with national and local code standards.

735

736 (3) Entry and/or Access Control Systems. If an entry and/or access control system is
737 integrated into an IDS, reports from the automated entry and/or access control system shall be
738 subordinate in priority to reports from intrusion alarms.

739

740 (4) Maintenance Mode. When the alarm zone is placed in the maintenance mode, this
741 condition shall be signaled automatically to the monitor station. The signal shall appear as an
742 alarm or maintenance message at the monitor station and the IDS shall not be securable while in
743 the maintenance mode. The alarm or message shall be continually visible at the monitor station
744 throughout the period of maintenance. A standard operating procedure shall be established to
745 address appropriate actions when maintenance access is indicated at the panel. All maintenance
746 periods shall be archived in the system. A self-test feature shall be limited to one second per
747 occurrence.

748

749 (5) Annunciation of Shunting or Masking Condition. Shunting or masking of any
750 internal zone or sensor shall be appropriately logged or recorded in archive. A shunted or
751 masked internal zone or sensor shall be displayed as such at the monitor station throughout the
752 period the condition exists whenever there is a survey of zones or sensors.

753

754 (6) Indications of Alarm Status. Indications of alarm status shall be revealed at the
755 monitoring station and optionally within the confines of the secure area.

756

757 (7) Power Supplies. Primary power for all IDE shall be commercial alternating or
758 direct current (AC or DC) power. In the event of commercial power failure at the protected area
759 or monitor station, the equipment shall change power sources without causing an alarm
760 indication.

761

762 (a) Emergency Power. Emergency power shall consist of a protected independent
763 backup power source that provides a minimum of 8 hours operating power battery and/or
764 generator power. When batteries are used for emergency power, they shall be maintained at full
765 charge by automatic charging circuits. The manufacturer's periodic maintenance schedule shall
766 be followed and results documented.

767

768 (b) Power Source and Failure Indication. An illuminated indication shall exist at
769 the PCU of the power source in use (AC or DC). Equipment at the monitor station shall indicate

770 a failure in power source, a change in power source, and the location of the failure or change.

771
772 (8) Component Tamper Protection. IDE components located inside or outside the
773 secure area shall be evaluated for a tamper protection requirement. If access to a junction box or
774 controller will enable an unauthorized modification, tamper protection shall be provided.

775
776 e. System Requirements

777
778 (1) Independent Equipment. When many alarmed areas are protected by one monitor
779 station, secure room zones shall be clearly distinguishable from the other zones to facilitate a
780 priority response. All sensors shall be installed within the protected area.

781
782 (2) Access and/or Secure Switch and PCU. No capability shall exist to allow changing
783 the access status of the IDS from a location outside the protected area. All PCUs shall be located
784 inside the secure area and should be located near the entrance. Assigned personnel shall initiate
785 all changes in access and secure status. Operations of the PCU may be restricted by use of a
786 device or procedure that verifies authorized use. In the secure mode, any unauthorized entry into
787 the space shall cause an alarm to be transmitted to the monitor station.

788
789 (3) Motion Detection Protection. Secure areas that reasonably afford access to the
790 security container or area where classified data is stored shall be protected with motion detection
791 sensors (e.g., ultrasonic and passive infrared). Use of dual technology is authorized when one
792 technology transmits an alarm condition independently from the other technology. A failed
793 detector shall cause an immediate and continuous alarm condition.

794
795 (4) Protection of Perimeter Doors. When an IDS is installed, each perimeter door shall
796 be protected by a balanced magnetic switch that meets UL Standard 634 (Reference (av)).

797
798 (5) Windows. All readily accessible windows (within 18 feet of ground level) shall be
799 protected by an IDS, either independently or by the motion detection sensors within the space,
800 whenever a secure room is located within a controlled compound or equivalent and forced entry
801 protection of the windows is not provided (also see subparagraph 1.b.(4) of this Appendix).

802
803 (6) IDS Requirements for Continuous Operations Facilities. A continuous operation
804 facility may not require an IDS. This type of secure area should be equipped with an alerting
805 system if the occupants cannot observe all potential entrances into the room. Duress devices may
806 also be required.

807
808 (7) False and/or Nuisance Alarm. Any alarm signal transmitted in the absence of
809 detected intrusion that is not identified as a nuisance alarm is a false alarm. A nuisance alarm is
810 the activation of an alarm sensor by some influence for which the sensor was designed but which
811 is not related to an intrusion attempt. All alarms shall be investigated and the results
812 documented. The maintenance program for the IDS shall ensure that incidents of false and/or
813 nuisance alarms shall not exceed 1 in a period of 30 days per zone.

814
815 f. Installation, Maintenance and Monitoring

816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861

(1) IDS Installation and Maintenance Personnel. Alarm installation and maintenance shall be accomplished by U.S. citizens who have been subjected to a trustworthiness determination according to Reference (1).

(2) Monitor Station Staffing. The monitor station shall be supervised continuously by U.S. citizens who have been subjected to a trustworthiness determination according to Reference (1).

3. ACCESS CONTROLS

a. The perimeter entrance to a secure facility (i.e., vault or secure room) shall be under control at all times during working hours to prevent entry by unauthorized personnel. This may be achieved by visual control or through use of an automated entry control system (AECS) that complies with the requirements of subparagraph 3.a.(2) of this section. Uncleared persons are to be escorted within the facility by a cleared person who is familiar with the security procedures of the facility. Personnel entering or leaving an area shall be required to secure the entrance or exit point. Authorized personnel who permit another individual to enter the area are responsible for confirming their need to know and access.

(1) Visual control may be accomplished by methods such as designated employees, guards, or continuously monitored closed circuit television.

(2) An AECS may be used if it meets the criteria stated in subparagraphs 3.a.(2)(a) and 3.a.(2)(b). The AECS shall identify an individual and authenticate the person's authority to enter the area through the use of an identification (ID) badge or card.

(a) The ID badge or key card shall use embedded sensors, integrated circuits, magnetic stripes, or other means of encoding data that identifies the facility and the individual to whom the card is issued.

(b) Biometrics verification identifies the individual requesting access by some unique personal characteristic and may be required for access to sensitive information. The Biometrics Identity Management Agency can provide further information regarding biometric technologies and capabilities. Personal characteristics that can be used for identity verification include:

1. Fingerprints
2. Hand geometry
3. Handwriting
4. Iris scans

862 5. Voice

863

864 6. Facial recognition

865

866 (3) In conjunction with subparagraph 3.a.(2)(a) of this section, a personal identification
867 number (PIN) may be required. The PIN shall be separately entered into the system by each
868 individual using a keypad device and shall consist of four or more digits, randomly selected, with
869 no known or logical association with the individual. The PIN shall be changed when it is
870 believed to have been compromised or subjected to compromise.

871

872 (4) Authentication of the individual's authorization to enter the area shall be
873 accomplished within the system by inputs from the ID badge and/or card, the personal identity
874 verification device, or the keypad with an electronic database of individuals authorized to enter
875 the area. A procedure shall be established for removing the individual's authorization to enter
876 the area upon reassignment, transfer, or termination, or when the individual's access is
877 suspended, revoked, or downgraded to a level lower than the required access level.

878

879 (5) Protection shall be established and maintained for all devices or equipment that
880 constitutes the entry control system. The level of protection may vary depending upon the type
881 of device or equipment being protected.

882

883 (a) Location where authorization data and personal identification or verification
884 data is input, stored, or recorded shall be protected.

885

886 (b) Card readers, keypads, communication or interface devices located outside the
887 entrance to a controlled area shall have tamper resistant enclosures and be securely fastened to
888 the wall or other permanent structure. Control panels located within a controlled area shall
889 require only a minimal degree of physical security protection sufficient to preclude unauthorized
890 access to the mechanism.

891

892 (c) Keypad devices shall be designed or installed in such a manner that an
893 unauthorized person in the immediate vicinity cannot observe the selection of input numbers.

894

895 (d) Systems that use transmission lines to carry access authorizations, personal
896 identification data, or verification data between devices or equipment located outside the
897 controlled area shall have line supervision.

898

899 (e) Electric strikes used in access control systems shall be heavy duty, industrial
900 grade.

901

902 (6) Access to records and information concerning encoded identification data and PINs
903 shall be restricted. Access to identification or authorizing data, operating system software or any
904 identifying data associated with the entry control system shall be limited to the fewest number of
905 personnel as possible. Such data or software shall be kept secure when unattended.

906

907 (7) Records shall be maintained reflecting active assignment of identification badge

908 and/or card, PIN, level of access, and similar system-related records. Records concerning
909 personnel removed from the system shall be retained for at least 90 days. Records of entries shall
910 be retained for at least 90 days or until investigations of system violations and incidents have
911 been resolved and recorded. Such records shall be destroyed when no longer required in
912 accordance with Reference (u) and DoD Component implementing directives and records
913 schedules.

914

915 **(8) *(Added)(DAF) The Office of the Under Secretary of Defense for Intelligence**
916 **memorandum, *Clarification of Automated Entry Control System Minimum Requirements*,**
917 **(reference (cp)) (or successor policy), explains that the technologies referenced in**
918 **paragraph 3.a(2)(b) for AECS minimum requirements are optional.**

919

920 b. The Heads of DoD Components may approve the use of standardized AECS that meet
921 the following criteria:

922

923 (1) For a Level 1 key card system (i.e., a key card bearing a magnetic stripe), the AECS
924 shall provide a .95 probability of granting access to an authorized user providing the proper
925 identifying information within three attempts. In addition, the system shall ensure an
926 unauthorized user is granted access with less than 0.05 probability after three attempts to gain
927 entry.

928

929 (2) For a Level 2 key card and PIN system (i.e., a key card bearing a magnetic stripe
930 used in conjunction with a PIN), the AECS shall provide a 0.97 probability of granting access to
931 an authorized user providing the proper identifying information within three attempts. In
932 addition, the system must ensure an unauthorized user is granted access with less than 0.010
933 probability after three attempts to gain entry have been made.

934

935 (3) For a Level 3 key card (i.e., a key card bearing a magnetic stripe used in conjunction
936 with a PIN and biometrics identifier system), the AECS shall provide a 0.97 probability of
937 granting access to an authorized user providing the proper identifying information within three
938 attempts. In addition, the system shall ensure an unauthorized user is granted access with less
939 than 0.005 probability after three attempts to gain entry have been made.

940

941 c. Electrical, mechanical, or electromechanical access control devices meeting the criteria
942 stated below, may be used to control access to secure areas during duty hours if the entrance is
943 under visual control. These devices are also acceptable to control access to compartmented areas
944 within a secure area. Access control devices shall be installed in the following manner:

945

946 (1) The electronic control panel containing the mechanism for setting the combination
947 shall be located inside the area. The control panel shall require only a minimal degree of
948 physical security designed to preclude unauthorized access to the mechanism.

949

950 (2) The control panel shall be installed, or have a shielding device mounted, so that an
951 unauthorized person in the immediate vicinity cannot observe the setting or changing of the
952 combination.

953

954 (3) An individual cleared at the same level as the highest classified information
955 controlled within the area shall select and set the combination.

956
957 (4) Electrical components, including wiring, or mechanical links (cables, rods, and so
958 on) shall be accessible only from inside the area, or, if they traverse an uncontrolled area, they
959 shall be secured within conduit to preclude surreptitious manipulation of components.

*(Added)(DAF) APPENDIX 2 TO ENCLOSURE 3

SECURITY CONTAINER AND VAULT DOOR VISUAL INSPECTION CHECKLIST

#	Inspection Item	Yes	Notes
1.0	Exterior of the Security Container		
1.1	Check to see if the General Services Administration (GSA) certification label is affixed		
1.2	Check for cracks, broken welds, tampering, and environment effects (e.g., rust, moisture, mold, corrosion)		
1.3	Check for modifications (e.g., repainting, alterations, unauthorized marking, camouflaged repairs, engraving)		
2.0	Release and Opening Drawer Mechanism		
2.1	Check for ease of operation		
2.2	Check the handle (should "spring back" when the bolt release is engaged)		
3.0	Drawers		
3.1	Check the alignment		
3.2	Check for ease of opening or closing operations (drawers should slide with no resistance)		
3.3	Check for debris on, or dryness or excessive lubrication of, sliding rails		
3.4	Check for missing screws		
3.5	Check for metal shavings on the ledge of the container where the drawer closes		
4.0	Vault Doors		
4.1	Check for cracks, broken welds, tampering, and environment effects (e.g., rust, moisture, mold, corrosion)		
4.2	Check for modifications (e.g., repainting, alterations, unauthorized marking, camouflaged repairs, engraving)		
4.3	Check bolt connections and hinges and non-removable hinge pins on outswing doors		
4.4	Check for ease of opening and closing operations		
4.5	Check alignment of door frame (door should swing open smoothly, without dragging or sagging)		
4.6	<i>Vault only:</i> Check to see if the GSA certification label is affixed		
5.0	High-Security Lock		
5.1	Ensure a Federal Standard FF-L-2740 combination lock is being utilized		
5.2	Check front/back of lock for alignment and looseness issues		
5.3	Check digital number display for clear visibility (e.g., showing partial numbers or skipping numbers)		
5.4	<i>Security Container Only:</i> Check behind the lock to ensure the drill plate and/or punch plate are intact <i>The drill plate is a thick piece of hardened metal usually found behind the lock; the punch plate is a thinner piece of hardened metal which slides into the groves behind the lock housing</i>		
5.5	Dial starts to pull away from the lock-base or lock is not soundly secured to the door		
5.6	Lock abruptly stops while spinning the dial		
5.7	Check operation of the emergency escape mechanism		
5.8	Other		

TRANSMISSION AND TRANSPORTATION

1
2
3
4
5
6 1. TRANSMISSION AND TRANSPORTATION PROCEDURES. Heads of the DoD
7 Components shall establish procedures for transmitting and transporting classified information that
8 maximizes the accessibility of classified information to individuals who are eligible for access
9 thereto and minimizes the risk of compromise while permitting the use of the most cost- effective
10 means. Persons transmitting or transporting classified information are responsible for ensuring that
11 the intended recipient(s) are authorized access, have a need to know, and have the capability to
12 store classified information in accordance with the requirements of this Manual.
13

14 a. COMSEC information shall be transmitted and transported according to NSA/CSS Policy
15 Manual 3-16 (Reference (av)).
16

17 b. NATO classified information, including NATO Restricted, shall be transmitted according
18 to the requirements of Reference (ab).
19
20

21 2. DISSEMINATION OUTSIDE THE DEPARTMENT OF DEFENSE
22

23 a. Classified information originating in another DoD Component or in a department or agency
24 other than the DoD may be disseminated to other DoD Components, to other U.S. departments or
25 agencies, or to a U.S. entity without the consent of the originating Component, department, or
26 agency, as long as:
27

28 (1) The criteria for access in section 3 of Enclosure 2 of this Volume are met.
29

30 (2) The classified information is NOT marked as requiring prior authorization for
31 dissemination to another department or agency. The marking "ORCON" may be used to identify
32 information requiring prior authorization for dissemination to another department or agency.
33

34 (3) The document was created ON or AFTER June 27, 2010, the effective date of
35 Reference (f) (however, also see paragraph 2.b of this section).
36

37 b. Documents created BEFORE June 27, 2010 may not be disseminated outside of the
38 Department of Defense without the originator's consent. Additionally, documents created on or
39 after June 27, 2010, whose classification is derived from documents created prior to that date, and
40 where the date before June 27, 2010 of the classified source(s) is readily apparent from the source
41 list, shall not be disseminated outside of the DoD without the originator's consent.
42

43 c. Classified information originating in, or provided to or by, the DoD may be disseminated to
44 a foreign government or an international organization of governments, or any element thereof, in
45 accordance with References (d), (f) and (z). See section 6 of this enclosure for further guidance.
46

47 d. Dissemination of information regarding intelligence sources, methods, or activities shall be
48 consistent with directives issued by the DNI.
49

50 e. Dissemination of classified information to state, local, tribal and private sector officials
51 pursuant to E.O. 13549 (Reference (aw)) shall be in accordance with implementing guidance issued
52 by the Department of Homeland Security.

53
54
55 3. TRANSMISSION OF TOP SECRET INFORMATION. Top Secret information shall be
56 transmitted only by:

57
58 a. Direct contact between appropriately cleared persons.

59
60 b. Electronic means over an approved secure communications system (i.e., a cryptographic
61 system authorized by the Director, NSA, or a protected distribution system designed and installed
62 to meet the requirements of National Security Telecommunications and Information Systems
63 Security Instruction (NSTISSI) 7003 (Reference (ax))). This applies to voice, data, message (both
64 organizational and e-mail), and facsimile transmissions.

65
66 c. The Defense Courier Service (DCS) if the material qualifies under the provisions of DoDI
67 5200.33 (Reference (ay)). The DCS may use a specialized shipping container as a substitute for a
68 DCS courier on direct flights if the shipping container is sufficiently constructed to provide
69 evidence of forced entry, secured with a high security padlock meeting Reference (ao)
70 specifications and equipped with an electronic seal that would provide evidence of surreptitious
71 entry. A DCS courier shall escort the specialized shipping container to and from the aircraft and
72 oversee its loading and unloading. This authorization also requires that the DCS develop
73 procedures that address protecting specialized shipping containers in the event a flight is diverted
74 for any reason.

75
76 d. Authorized U.S. Government agency courier services (e.g., Department of State Diplomatic
77 Courier Service, authorized DoD Component courier service).

78
79 e. Appropriately cleared U.S. Military and Government civilian personnel specifically
80 designated to carry the information and traveling by surface transportation.

81
82 f. Appropriately cleared U.S. Military and Government civilian personnel specifically
83 designated to carry the information and traveling on scheduled commercial passenger aircraft
84 within and between the U.S., its territories, and Canada.

85
86 g. Appropriately cleared U.S. Military and Government civilian personnel specifically
87 designated to carry the information and traveling on scheduled commercial passenger aircraft on
88 flights outside the U.S., its territories, and Canada.

89
90 h. DoD contractor employees with appropriate clearances traveling within and between the
91 United States and its territories provided the requirements of Reference (w) and DoDM 5220.22
92 (Reference (az)) are met.

93
94 **i. (Added)(DAF) For transmission of top secret information, the sender shall use the AF**
95 **Form 310, *Document Receipt and Destruction Certificate*, except when transmitted over**
96 **electronic means on an approved secure communications system, or when it is hand-carried**
97 **and transferred to another authorized individual. (T-1). The receiver shall complete and**
98 **return the AF Form 310 within 15 business days inside the U.S., or 30 business days outside**

99 **the U.S. for any transmitted material. (T-1). The sender should contact the servicing IP**
100 **office (or PSO and SSO, if applicable) for assistance if the receiver cannot verify receiving the**
101 **transmitted material.**

102
103
104 4. TRANSMISSION OF SECRET INFORMATION. Secret information may be transmitted by:

105
106 a. Any of the means approved for the transmission of top secret information.

107
108 b. Appropriately cleared contractor employees if the transmission meets the requirements
109 specified in References (w) and (az).

110
111 c. Overnight delivery, provided the requirements of this paragraph are met. Heads of DoD
112 Components may, when a requirement exists for overnight delivery to a DoD Component within
113 the U.S. and its territories, authorize the use of the current holder of the GSA contract for overnight
114 delivery of information for the Executive Branch as long as applicable postal regulations (chapter I
115 of title 39, CFR (Reference(bb))) are met. Any such delivery service shall be U.S. owned and
116 operated, provide automated in-transit tracking of the classified information, and ensure package
117 integrity during transit. The contract shall require cooperation with U.S. Government inquiries in
118 the event of a loss, theft, or possible compromise. The sender is responsible for ensuring that an
119 authorized person at the receiving end is aware that the package is coming and will be available to
120 receive the package, verifying the mailing address is correct, and confirming (by telephone or e-
121 mail) that the package did in fact arrive within the specified time period. The package may be
122 addressed to the recipient by name. The release signature block on the receipt label shall not be
123 executed under any circumstances. The use of external (street side) collection boxes is prohibited.
124 Classified COMSEC information, NATO information, SCI, and FGI shall not be transmitted in this
125 manner. See Multiple Award Schedule 48, "Transportation, Delivery and Relocation Solutions," on
126 the GSA eLibrary Website (<http://www.gsaelibrary.gsa.gov/ElibMain/home.do>) for a listing of
127 commercial carriers authorized for use under the provisions of this paragraph.

128
129 d. U.S. Postal Service registered mail within and between the U.S., the District of Columbia,
130 and the Commonwealth of Puerto Rico.

131
132 e. U.S. Postal Service Express mail within and between the 50 States, the District of
133 Columbia, and the Commonwealth of Puerto Rico. The "Waiver of Signature and Indemnity"
134 block on the U.S. Postal Service Express Mail Label 11-B may not be executed under any
135 circumstances. The use of external (street side) Express Mail collection boxes is prohibited.

136
137 f. U.S. Postal Service and Canadian registered mail with registered mail receipt between
138 U.S. Government and Canadian government installations in the U.S. and Canada.

139
140 g. U.S. Postal Service registered mail through Military Postal Service facilities outside the
141 United States and its territories, if the information does not at any time pass out of U.S. citizen
142 control and does not pass through a foreign postal system or any foreign inspection.

143
144 h. Carriers cleared under the National Industrial Security Program providing a protective
145 security service. This method is authorized only within the continental U.S. (CONUS) when other
146 methods are impractical, except that this method is also authorized between U.S. and Canadian
147 government approved locations documented in a transportation plan approved by U.S. and

148 Canadian government security authorities.

149
150 i. U.S. Government and U.S. Government contract vehicles including aircraft, ships of the
151 U.S. Navy, civil service-operated U.S. Naval ships, and ships of U.S. registry. Appropriately
152 cleared operators of vehicles, officers of ships or pilots of aircraft who are U.S. citizens may be
153 designated as escorts provided the control of the carrier is maintained on a 24-hour basis. The
154 escort shall protect the shipment at all times, through personal observation or authorized storage to
155 prevent inspection, tampering, pilferage, or unauthorized access. Observing the shipment is not
156 required during flight or sea transit, provided it is loaded into a compartment that is not accessible
157 to any unauthorized persons or in a specialized secure, safe-like container.

158
159 j. Air carrier without an appropriately cleared escort to locations outside the U.S. and its
160 territories, provided the provisions of this paragraph are met. In exceptional circumstances, with
161 the written approval of the sending and receiving government DSAs, material may be transmitted
162 outside the U.S. and its territories without an appropriately cleared escort provided the following
163 criteria are met:

164
165 (1) The material is stored in the hold of an aircraft of an U.S. owned or registered air
166 carrier or an air carrier owned by or under the registry of the recipient government.

167
168 (2) The shipment is placed in a compartment that is not accessible to any unauthorized
169 person or in a specialized shipping container approved for this purpose.

170
171 (3) The air carrier agrees in writing to permit a cleared DoD or cleared U.S. company
172 employee, specifically designated by name, to observe placement of the classified shipment into
173 the aircraft.

174
175 (4) The flight is direct between two designated points with no intermediate stops.

176
177 (5) The air carrier agrees in writing that a designated officer on the aircraft will assume
178 responsibility for the classified material while in route to the destination.

179
180 (6) Written emergency instructions are provided to the air carrier.

181
182 (7) Arrangements are made for recipient foreign government officials, the designated
183 government representative (DGR), or other recipient government representative, designated by
184 name and organization, in writing, to be present at the unloading of the consignment and
185 immediately assume security control for the recipient government.

186
187 (8) The foregoing requirements are documented in the transportation plan.

188
189 (9) The exceptional circumstances are documented in the request for exception.

190
191 **k. (Added)(DAF) For transmission of classified information, secret and below, the**
192 **sender shall use the AF Form 310, except when transmitted over electronic means on an**
193 **approved secure communications system, or when it is hand-carried and transferred to**
194 **another authorized individual. (T-1). The receiver shall complete and return the AF Form**
195 **310 within 15 business days inside the U.S., or 30 business days outside the U.S. for any**
196 **transmitted material. (T-1). The sender should contact the servicing IP office (or PSO and**

197 **SSO, if applicable) for assistance if the receiver cannot verify receiving the transmitted**
198 **material.**

200
201 5. TRANSMISSION OF CONFIDENTIAL INFORMATION. Confidential information may be
202 transmitted by:

203
204 a. Any of the means approved for the transmission of secret information.

205
206 b. U.S. Postal Service Registered Mail for:

207
208 (1) Material to and from military post office addressees (i.e., Fleet Post Office or Army
209 Post Office) located outside the U.S. and its territories.

210
211 (2) Material when the originator is uncertain that the addressee's location is within U.S.
212 boundaries.

213
214 c. U.S. Postal Service certified mail (or registered mail, if required above) for material
215 addressed to DoD contractors or non-DoD agencies.

216
217 d. U.S. Postal Service first class mail between DoD Component locations anywhere in the
218 United States and its territories. The outer envelope or wrapper shall be endorsed: "Return Service
219 Requested."

220
221 e. Commercial carriers that provide a constant surveillance service, as defined in Reference
222 (w), within CONUS.

223
224 f. Commanders or masters of ships of U.S. registry who are U.S. citizens. Confidential
225 information shipped on ships of U.S. registry may not pass out of U.S. Government control. The
226 commanders or masters shall sign a receipt for the material and agree to:

227
228 (1) Deny unauthorized persons access to the confidential material, including customs
229 inspectors, with the understanding that confidential cargo that would be subject to customs
230 inspection shall not be unloaded.

231
232 (2) Maintain control of the cargo until a receipt is obtained from an authorized
233 representative of the consignee.

234
235 g. Alternative or additional methods of transmission the Head of the DoD Component
236 approves.

237
238
239 6. TRANSMISSION OF CLASSIFIED INFORMATION AND MATERIAL TO FOREIGN
240 GOVERNMENTS. Classified information and material approved for release to a foreign
241 government or international organization (collectively "foreign governments") according to
242 Reference (y) shall be transmitted between representatives of each government through
243 government-to-government channels or through other channels agreed to in writing by the DSAs of
244 the sending and receiving governments. International transfers of classified material shall comply
245 with this enclosure, its appendix, and the following:

246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294

a. U.S. Government control and accountability of classified information or material shall be maintained from the point of origin to the ultimate destination, until it is officially transferred to the intended recipient government through its DGR.

b. In urgent situations, appropriately cleared U.S. Government agency employees may be authorized to hand-carry classified material in accordance with this enclosure and its appendix.

c. Each DoD Component entering into a contract or an international agreement that will entail the transfer of classified information and material to a foreign government shall consult with supporting DoD transportation and security authorities to confirm the appropriate transfer arrangements and establish responsibilities for the transfer arrangements prior to the execution of the agreement or contract.

7. SECURITY REQUIREMENTS FOR TRANSFERS OF DEFENSE ARTICLES TO AUSTRALIA OR THE UNITED KINGDOM WITHOUT AN EXPORT LICENSE OR OTHER WRITTEN AUTHORIZATION

a. Background. The Defense Trade Cooperation Treaty between the United States and Australia, which was signed by the U.S. on September 5, 2007, and the Defense Trade Cooperation Treaty between the U.S. and the United Kingdom (UK), which was signed by the U.S. on June 21, 2007, provide comprehensive frameworks for exports and transfers of certain classified and unclassified defense articles, without an export license or other written authorization to Australian Communities and UK Communities respectively (see Glossary). The provisions of the treaties apply to both government organizations and contractors. This section provides implementing guidance to DoD entities that are eligible to export certain classified and unclassified defense articles.

b. Applicability. Defense articles (defined in Glossary) fall under the scope of the treaties when they are in support of:

(1) U.S. and Australia or UK, as applicable, combined military or counter- terrorism operations;

(2) U.S. and Australia or UK, as applicable, cooperative security and defense research, development, production, and support programs;

(3) Mutually determined specific security and defense projects where the Government of Australia or Government of the UK, as applicable, is the end-user; or

(4) U.S. Government end-use.

c. Markings. Prior to transfer to Australia or the UK, defense articles that fall under the scope of these treaties must be labeled, as applicable, with an overall marking as directed in subparagraph 7.c.(1) or 7.c.(2) of this enclosure. While these markings do not generally conform to the marking standard specified in Volume 2 of this Manual, the markings are required by these Defense Trade Cooperation Treaties and their Implementing Arrangements and must be used as specified.

(1) Markings required for transfer of defense articles to Australia:

(a) Classified U.S. defense articles shall be marked:

1. CLASSIFICATION LEVEL USML//REL TO USA, AUS TREATY COMMUNITY.

2. For example, for defense articles classified SECRET, the marking shall be “SECRET USML//REL TO USA, AUS TREATY COMMUNITY.” Apply other applicable classification markings (e.g., classification authority block, portion markings, or other dissemination markings) in accordance with Volume 2 of this Manual.

(b) Unclassified U.S. defense articles shall be marked:

1. //RESTRICTED USML//REL TO USA, AUS TREATY COMMUNITY.

(c) When defense articles are returned from Australia to the U.S., any defense articles marked as RESTRICTED in this manner purely for the purposes of the treaty will be considered to be unclassified and such markings shall be removed.

(2) Markings required for transfer of defense articles to the UK:

(a) Classified U.S. defense articles shall be marked:

1. CLASSIFICATION LEVEL USML//REL TO USA, GBR TREATY COMMUNITY.

2. For example, for defense articles classified SECRET, the marking shall be “SECRET USML//REL TO USA, GBR TREATY COMMUNITY.” Apply other applicable classification markings (e.g., classification authority block, portion markings, or other dissemination markings) in accordance with Volume 2 of this Manual.

(b) Unclassified U.S. defense articles shall be marked:

1. //RESTRICTED USML//REL TO USA, GBR TREATY COMMUNITY.

(c) When defense articles are returned from the UK to the U.S., any defense articles marked as RESTRICTED in this manner purely for the purposes of the treaty will be considered to be unclassified and such marking shall be removed.

(3) The following notice shall be included (e.g., as part of the bill of lading) whenever defense articles are exported in accordance with the provisions of these treaties: “These U.S. Munitions List commodities are authorized by the U.S. Government under the U.S.-[Australia or United Kingdom, as applicable] Defense Trade Cooperation Treaty for export only to [Australia or United Kingdom, as applicable] for use in approved projects, programs or operations by members of the [Australian or United Kingdom, as applicable] Community. They may not be retransferred or re-exported or used outside of an approved project, program, or operation, either in their original form or after being incorporated into other end-items, without the prior written approval of the U.S. Department of State.”

344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392

(4) The items to be marked are:

(a) Defense articles (other than technical data) shall be individually labeled with the appropriate marking detailed in paragraphs 7.c.(1) or 7.c.(2) of this section; or, where such labeling is impracticable (e.g., propellants, chemicals), shall be accompanied by documentation clearly associating the defense articles with the appropriate markings as detailed in paragraphs 7.c.(1) or 7.c.(2) of this section.

(b) Technical data (including technical papers, manuals, presentations, specifications, guides and reports), regardless of media or means of transmission (physical, oral, or electronic), shall be individually labeled with the appropriate marking detailed in paragraphs 7.c.(1) or 7.c.(2) of this section; or, where such labeling is impracticable shall be accompanied by documentation or verbal notification clearly associating the technical data with the appropriate markings as detailed in paragraphs 7.c.(1) or 7.c.(2) of this section.

d. Transfers

(1) All defense articles that fall under the scope of the treaty must be transferred from the U.S. point of embarkation through channels approved by both the U.S. and, as appropriate, Australia or the UK.

(2) For transfers of defense articles as freight, the contractor shall prepare a transportation plan in accordance with section 10 of the Appendix to Enclosure 4 of this Volume. For transfer of classified U.S. defense articles, a freight forwarder must have a valid facility security clearance and storage capability at the appropriate level. For unclassified U.S. defense articles that are transferred as freight, a freight forwarder is not required to be cleared.

8. USE OF SECURE COMMUNICATIONS FOR TRANSMISSION OF CLASSIFIED INFORMATION. Transmission of DoD information shall comply, as appropriate, with the COMSEC measures and procedures identified in DoDI 8523.01 (Reference (bb)).

a. Computer-to-Computer Transmission. In addition to meeting the requirements of paragraph 3.b of this enclosure, computer and other IT systems used for transmitting classified information shall be approved and accredited in accordance with Reference (s) or Intelligence Community Directive 503 (Reference (bc)), as applicable, to operate at a level of classification commensurate with the data being transmitted. Electronic transmission of classified information over secure computer-to-computer links (e.g., via secure e-mail) is preferable to physical transfer of hard copy documents. Classified information transmitted in this manner shall be marked in accordance with Volume 2 of this Manual.

b. Facsimile (Fax) Transmission. Only secure facsimile equipment shall be used for facsimile transmission of classified information. The following procedures shall be followed:

(1) The individual transmitting the information shall ensure the recipient has the appropriate clearance and a need to know, and that the secure connection is at the appropriate level of classification for the information being transmitted.

393 (2) Header or coversheets used to precede the transmission of classified material shall be
394 conspicuously marked with the highest security classification of the transmitted information and
395 any required control markings. The coversheet shall also include the originator's name,
396 organization, phone number, an unclassified title, the number of pages, and the receiver's name,
397 organization and phone number. When the coversheet contains no classified information, it shall
398 also note "Unclassified when Classified Attachment(s) Removed."
399

400 (3) Documents transmitted by fax shall have all markings required for a finished
401 document, and shall be controlled and safeguarded by the recipient accordingly.
402

403 c. Telephone. Only approved secure telephones, including cell phones and phones integral to
404 personal electronic devices, authorized by the Director, NSA pursuant to paragraph 3.b of this
405 enclosure, may be used for telephonic transmission of classified information. Users must ensure
406 the secure connection is at the appropriate level of classification for the information being
407 discussed.
408

409
410 9. SHIPMENT OF BULK CLASSIFIED MATERIAL AS FREIGHT. Procedures established for
411 shipping bulk classified material as freight shall include provisions for shipping material in closed
412 vehicles when required, appropriate notice to the consignee concerning the shipment, procedures at
413 transshipment activities, and actions to be taken in the case of non-delivery or unexpected delay in
414 delivery.
415

416
417 10. PREPARATION OF MATERIAL FOR SHIPMENT. When transferring classified
418 information, it shall be enclosed in two opaque, sealed envelopes, wrappings, or containers, durable
419 enough to properly protect the material from accidental exposure and facilitate detection of
420 tampering.
421

422 a. Prepare, package, and securely seal classified material in ways that minimize risk of
423 accidental exposure or undetected deliberate compromise. To minimize the risk of exposure of
424 classified information, package documents so that classified material is not in direct contact with
425 the inner envelope or container (e.g., fold so classified material faces together).
426

427 (1) Address the outer envelope or container to an official U.S. Government activity or to a
428 DoD contractor with a facility clearance and appropriate storage capability and show the complete
429 return address of the sender. Do not address the outer envelope to an individual. Office codes or
430 phrases such as "Attention: Research Department" may be used.
431

432 (2) Show the address of the receiving activity, the address of the sender, the highest
433 classification of the contents (including, where appropriate, any special dissemination or control
434 markings such as "Restricted Data" or "NATO"), and any applicable special instructions on the
435 inner envelope or container. The inner envelope may have an attention line with a person's name.
436

437 (3) Do not place a classification marking or any other unusual marks on the outer
438 envelope or container that might invite special attention to the fact that the contents are classified.
439

440 (4) Address classified information intended only for U.S. elements of international staffs
441 or other organizations specifically to those elements.

442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490

b. When classified material is hand-carried outside an activity, a locked briefcase or zippered pouch may serve as the outer wrapper. In such cases, the addressing requirements of subparagraph 10.a.(1) of this section do not apply. Refer to section 11 of this enclosure for additional requirements on use of briefcases and pouches.

c. If the classified material is an accessible internal component of an item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information.

d. If the classified material is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered a sufficient enclosure provided observation of it does not reveal classified information.

e. If the classified material is an item of equipment that cannot be packaged and the shell or body is classified, it shall be concealed with an opaque covering hiding all classified features.

f. Specialized shipping containers, including closed cargo transporters, may be considered the outer wrapping or cover.

11. USE OF BRIEFCASES OR ZIPPERED POUCHES FOR HAND-CARRYING CLASSIFIED MATERIAL. A locked briefcase or zippered pouch made of canvas or other heavy-duty material and having an integral key-operated lock may be used for hand-carrying classified material outside an activity. Such cases may also be used to restrict access to classified material when the intended recipient is not immediately available. If using a briefcase or pouch to hand-carry classified material outside an activity, or in any circumstance when the possibility exists that the briefcase or pouch shall be left for subsequent opening by the intended recipient, package the material as required by section 10 of this enclosure and additionally observe the following procedures:

a. Clearly and recognizably display the name and street address of the organization sending the classified material, and the name and telephone number of a point of contact within the sending activity, on the outside of the briefcase or pouch.

b. Serially number the pouch or briefcase and clearly display this serial number on its exterior surface.

c. Lock the briefcase or pouch and place its key in a separate sealed envelope.

d. Store the briefcase or pouch, when containing classified material, according to the highest classification level and any special controls applicable to its contents.

e. Ensure the activity authorizing use of the briefcase or pouch maintains an internal system to account for and track the location of the pouch and its key.

f. Use a briefcase or pouch only to assist in enforcing need to know. Its use shall in no way abrogate personal responsibility to ensure that the classified material is delivered to a person who has an appropriate security clearance and access for the information involved.

491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539

12. ESCORT, COURIER, OR HAND-CARRY OF CLASSIFIED MATERIAL

a. Authority. Appropriately cleared and briefed personnel may be authorized to escort or carry classified material between locations when other means of transmission or transportation cannot be used. The Heads of the DoD Components shall establish procedures to ensure that hand-carrying of classified material is minimized to the greatest extent possible and does not pose unacceptable risk to the information. Hand carrying may be authorized only when:

(1) The information is not available at the destination and operational necessity or a contractual requirement requires it.

(2) The information cannot be sent via a secure e-mail, facsimile transmission or other secure means.

(3) The appropriate official authorizes the hand-carry according to procedures the Head of the DoD Component establishes.

(4) The hand-carry is accomplished aboard a U.S. carrier, or a foreign carrier if no U.S. carrier is available, and the U.S. escort retains custody and physical control of the information at all times.

(5) Arrangements have been made for secure storage of the information at a U.S. Government or cleared U.S. contractor facility.

b. Packaging Requirements. Classified material that is hand-carried shall be packaged in the same manner as described in section 10 of this enclosure for material being shipped.

c. Responsibilities. Individuals hand carrying or serving as couriers or escorts for classified information shall be informed of, and acknowledge, their security responsibilities. These requirements may be satisfied by a briefing or by requiring the individual to read written instructions that state the following responsibilities:

(1) The individual is liable and responsible for the material being carried or escorted.

(2) The material is not, under any circumstances, to be left unattended. During overnight stops arrangements shall be made for storage of the classified material at a U.S. military facility, embassy, or cleared contractor facility. Classified information shall not be stored in hotel safes.

(3) The material shall not be opened in route except in the circumstances described in paragraph 12.d of this section.

(4) The material shall not be discussed or disclosed in any public place.

(5) The individual shall not deviate from the authorized travel schedule.

(6) In cases of emergency, the individual shall take measures to protect the material.

(7) The individual is responsible for ensuring that personal travel documents (passport,

540 courier authorization (if required), medical documents, etc.) are complete, valid, and current.

541
542 d. Customs, Police, or Immigration Officials. Arrangements shall be made in advance with
543 customs, police or immigration officials to facilitate movement through security. However, there is
544 no assurance of immunity from search by the customs, police, or immigration officials of countries,
545 including the U.S., whose border the courier may cross. Therefore, if such officials inquire into the
546 contents of the consignment, the courier shall present the courier authorization or orders and ask to
547 speak to the senior customs, police, or immigration official. This action shall normally suffice to
548 pass the material through unopened. However, if the senior official demands to see the actual
549 contents of the package, it may be opened in his or her presence, but shall be done in an area out of
550 sight of the public. In that instance:

551
552 (1) Precautions shall be taken to show officials only as much of the contents as satisfies
553 them that the package does not contain any other item. The courier shall ask the official to repack
554 the material or assist in repacking it immediately upon completing the examination.

555
556 (2) The senior customs, police, or immigration official shall be requested to provide
557 evidence of opening and inspection of the package by sealing and signing it when closed and
558 confirming on the shipping documents (if any) or courier certificate that the package has been
559 opened. Both the addressee and the dispatching security officer shall be informed in writing of the
560 opening of the material.

561
562 (3) Classified material to be carried by a courier shall be inventoried, a copy of the
563 inventory shall be retained at the courier's office or duty location, and the courier shall carry a
564 copy.

565
566 (4) Upon return, the courier shall return all classified material in a sealed package or, for
567 any classified material that is not returned, produce a receipt signed by the security officer of the
568 addressee organization.

569
570 (5) For guidance on hand-carrying NATO classified material, see Reference (ab).

571
572 e. Disclosure Authorization. In the event that the hand-carry of classified information shall
573 also involve the disclosure of such information to foreign nationals, the DoD Component official
574 responsible for approving the hand-carry is also responsible for ensuring a disclosure authorization
575 is obtained in accordance with Reference (y).

576
577
578 13. ESCORT, COURIER, OR HAND-CARRY AUTHORIZATION. Responsible officials, as
579 determined by DoD Component procedures, shall provide a written statement to each individual
580 who is authorized to escort, courier, or hand-carry classified material. Procedures for authorizing
581 on-site contractors to escort, courier, or hand-carry classified material shall comply with the
582 requirements of References (w) and (az). Authorization to escort, courier, or hand-carry SCI shall
583 be in accordance with Reference (i).

584
585 a. The authorization statement may be contained in a letter, a courier card, or other written
586 document, including travel orders. For travel aboard commercial aircraft, section 14 of this
587 enclosure also applies. For international travel, also see the Appendix to this enclosure.

589 b. DD Form 2501, "Courier Authorization," may be used to identify appropriately cleared
590 DoD military and civilian personnel who have been approved to hand-carry classified material
591 according to the following:

592
593 (1) The individual has a recurrent need to hand-carry classified information.

594
595 (2) An appropriate official in the individual's servicing security office signs the form.

596
597 (3) The form is issued for no more than 2 years at a time. The requirement for
598 authorization to hand-carry classified information shall be reevaluated and/or revalidated at least
599 once every 2 years, and a new form issued, if appropriate.

600
601 (4) Only the last four (4) digits of the individual's social security number shall be used in
602 completing the DD Form 2501. Currently valid DD Forms 2501 shall be updated when renewed.

603
604 (5) The use of the DD Form 2501 for verification of authorization to hand-carry SCI or
605 SAP information shall be according to policies and procedures established by the official having
606 security responsibility for such information or programs.

607
608
609 14. HAND-CARRYING OR ESCORTING CLASSIFIED INFORMATION ON COMMERCIAL
610 AIRCRAFT. Although pre-coordination is not typically required, in unusual situations advance
611 coordination with the local Transportation Security Administration (TSA) field office may be
612 warranted to facilitate clearance through airline screening processes.

613
614 a. The individual designated as courier shall possess a DoD or contractor-issued identification
615 card and a government-issued photo identification card (if at least one of the identification cards
616 does not contain date of birth, height, weight, and signature, include these items in the written
617 authorization).

618
619 b. The courier shall have a courier card or authorization letter prepared on letterhead
620 stationery of the agency authorizing the carrying of classified material, which shall:

621
622 (1) Give the full name of the individual and his or her employing agency or company.

623
624 (2) Carry a date of issue and an expiration date.

625
626 (3) Carry the name, title, signature, and phone number of the official issuing the letter.

627
628 (4) Carry the name of the person and official U.S. Government telephone number of the
629 person designated to confirm the courier authorization.

630
631 c. Upon arrival at the screening checkpoint the individual designated as courier shall ask to
632 speak to the TSA Supervisory Transportation Security Officer and shall present the required
633 identification and authorization documents. If the courier does not present all required documents,
634 including valid courier authorization, DoD or contractor-issued identification card, and
635 government-issued photo identification card, TSA officials will require the classified material to be
636 screened in accordance with their standard procedures.

637

638 d. The courier shall go through the same airline ticketing and boarding process as other
639 passengers. When the TSA Supervisory Transportation Security Officer confirms the courier's
640 authorization to carry classified material, only the U.S. Government classified material is exempted
641 from any form of inspection; the courier and all of the courier's personal property shall be provided
642 for screening. The classified material shall remain within the courier's sight at all times during the
643 screening process. When requested, the package(s) or the carry-on luggage containing the
644 classified information may be presented for security screening so long as the courier maintains
645 visual sight and the packaging or luggage is not opened.

646
647 e. Hand-carrying items aboard international commercial aircraft shall be done only on an
648 exception basis. DoD travelers requiring access to classified materials at an overseas location shall
649 exhaust all other transmission options (e.g., electronic file transfer, advance shipment by courier)
650 before hand-carrying items aboard international commercial aircraft. See also sections 12 and 13,
651 paying particular attention to paragraph 12.d. In addition to the requirements in the subparagraphs
652 above, for international travel the authorization letter shall describe the material being carried (e.g.,
653 "three sealed packages (9" x 8" x 24")," addressee and sender) and the official who signed the
654 authorization letter shall sign each package or carton to be exempt to facilitate its identification.

655

656

657 Appendix

658 Transfer of Classified Information or Material to Foreign Governments

APPENDIX TO ENCLOSURE 4TRANSFER OF CLASSIFIED INFORMATION OR MATERIAL TO FOREIGN GOVERNMENTS1. GENERAL

a. Transfers of classified information and material to a foreign government or international organization (hereinafter, "foreign government") may occur in the U.S., in the recipient country, or in a third country. The risks of loss or compromise increase when classified information and material are transferred across international borders. Therefore, transfer arrangements must be thorough and clearly written. They must be understood and agreed to by the sending and receiving government officials involved in the transfer.

b. Transfers shall occur between government officials through official government-to-government channels (e.g., U.S. Government military transportation, Military Postal Service registered mail, DCS, the DTS). However, in some cases, it may not be possible to transfer the information and material through official government-to-government channels; the use of other channels may be necessary. These other channels may involve transfers by hand carrying or secure communications between cleared contractors or the use of cleared freight forwarders and commercial carriers.

c. Classified information or material, approved for disclosure in accordance with Reference (y), to be transferred to a foreign government or its representative shall be transferred only to a person or organization designated by the recipient government to sign for and assume custody and responsibility on behalf of the government. This designation should be in a letter of offer and acceptance (LOA), in a program agreement/arrangement or implementing procedures, in a contract, or in a visit authorization. The designation shall contain assurances that the person to receive the information or material will have a security clearance at the appropriate level, that the person shall assume full security responsibility for the material on behalf of the foreign government, and that the information will be protected in accordance with the governing agreement or arrangement.

d. If other than government-to-government channels are to be used to transfer classified information or material to a foreign government, written transfer arrangements shall be approved by the DSAs of the sending and receiving governments, unless authority is delegated by a DSA, in writing, to a DGR of the respective sending or receiving government. The written arrangements shall provide for a DoD DGR or other DoD official to exercise oversight and ensure secure transfer from the point of origin to the ultimate destination, or to another agreed location where the recipient government's representative assumes responsibility. The information or material transferred shall be classified no higher than Secret.

e. Each LOA, agreement, contract, or other arrangement involving the disclosure or release of classified information or material to foreign governments shall either contain detailed transfer instructions or require that the DoD Component sponsoring the transaction and the recipient government prepare and approve a separate plan for transferring the information or material. See section 10 of this appendix for required transportation plan content. If classified information or

708 material is to be transferred from a non-governmental entity to a foreign government, it is also
709 subject to the requirement of Reference (x).

710
711 f. U.S. Government communications and IT systems used for the transfer of classified
712 information to foreign governments shall comply with paragraph 8.a. of Enclosure 4 of this
713 Volume.

714
715 g. The requirements of this appendix do not pertain to:

716
717 (1) The disclosure or release of intelligence information and products under the purview of
718 the DNI. Such disclosure or release shall be governed by policy issued by the DNI.

719
720 (2) Transfers of classified information and material during visits, which shall comply with
721 Reference (q) and paragraph C3.2.7.6 of the DoD Foreign Clearance Manual (Reference (be)).

722
723
724 2. RECEIPTS. Receipts are required for all transfers of classified information and material to a
725 foreign government, except as noted in paragraphs 2.a. and 2.b. of this section. The receipts serve
726 two important purposes. First, they document the transfer of security jurisdiction between the
727 governments. Second, they alert the recipient government that the information or material has been
728 transferred, and that it is responsible for protecting the information or material in compliance with
729 the pertinent security or program agreement or arrangement.

730
731 a. Most foreign governments waive the receipt requirement for their restricted information.

732
733 b. Transmissions of classified information to a foreign government by IT and communications
734 systems meeting the requirements of paragraph 1.f. of this appendix shall, at a minimum, be
735 audited to assure that the intended recipient receives the information. The audit procedures for
736 verifying receipt shall be commensurate with those specified in DoDI 8500.2 (Reference (v)).

737
738
739 3. TRANSFERS BY DOD COMPONENT COURIER SERVICE, HAND-CARRYING, OR
740 POSTAL SERVICE. Classified material that is of such size, weight, and configuration that it is
741 suitable for transfer by an official DoD Component courier service, by a DoD employee approved
742 to hand-carry classified information or material, or by U.S. Postal Service or Military Postal
743 Service registered mail, shall be transferred in compliance with Enclosure 4 of this volume, and
744 shall be delivered or addressed to:

745
746 a. An embassy, consulate, or other official agency of the recipient government having
747 extraterritorial status in the U.S.; or

748
749 b. A U.S. Embassy or a U.S. military organization in the recipient country or in a third-party
750 country for delivery to a DGR or other designated representative of the recipient government.

751
752
753 4. TRANSFERS OF CLASSIFIED INFORMATION OR MATERIAL AS FREIGHT

754
755
756 a. Foreign Military Sales (FMS). DoD officials authorized to approve an FMS transaction

757 involving the delivery of U.S. classified material to a foreign government shall, prior to any
758 commitment on transfer arrangements, consult with supporting transportation officials to determine
759 if secure U.S. Government transportation is available through U.S. Transportation Command or
760 other DoD transportation authorities (e.g., Surface Deployment and Distribution Command,
761 Military Sealift Command, Air Mobility Command) from the CONUS point of origin to the
762 ultimate foreign destination, and to facilitate other modes of transfer when U.S. Government
763 transportation is not available. Normally, the U.S. shall use the DTS to deliver classified material
764 resulting from FMS to the recipient government. The DoD Component FMS implementing agency
765 that prepares the LOA shall develop a transportation plan in coordination with the foreign
766 government. A generic transportation plan, containing standard security requirements necessary
767 for any transfer, should be prepared during LOA negotiation. The LOA should specify
768 responsibilities for completing the plan prior to the transfer of material. Security and transportation
769 officials supporting the implementing agency shall evaluate and approve the transportation plan, in
770 accordance with requirements of DoD 5105.38-M (Reference (be)). If the plan is not satisfactory,
771 the implementing agency will require that transfers be delayed until the plan is satisfactory.
772

773 b. Direct Commercial Sales. In accordance with Reference (x), transfers of classified material
774 resulting from direct commercial sales shall comply with the same security standards that apply to
775 FMS transfers, including the preparation of a generic transportation plan during contract
776 negotiations.
777

778 c. Cooperative Programs. Transfer of classified information or material in support of a
779 cooperative program shall be through official government-to-government channels or through other
780 channels as agreed to by the respective governments (government-to-government transfer).
781

782 **d. (Added)(DAF) Each LOA involving the transfer of classified information, software or**
783 **critically controlled assets to foreign governments, shall contain a detailed security plan**
784 **designating the security protection requirements. (T-0). Consistent with the SAMM, Table**
785 **C4.T1, *Presidential Determination Criteria for FMS Eligibility*, for cases involving FMS**
786 **classified information, contingency construction authority must be consistent with providing**
787 **protection at substantially the same degree of security as provided by the USG. (T-0).**
788
789

790 5. DELIVERY WITHIN THE UNITED STATES. Delivery of classified information or material
791 to a foreign government at a point within the U.S., using carriers specified in Enclosure 4 for the
792 level of classified information or material involved, shall take place at:
793

794 a. An embassy, consulate, or other official agency under the control of the recipient
795 government. An official designated by the foreign government as its DGR shall sign for the
796 consignment.
797

798 b. The point of origin. When a DGR or other representative designated by the recipient
799 government accepts delivery of classified material at the point of origin (e.g., a manufacturing
800 facility or depot), the DoD DGR or other designated DoD official who transfers custody shall
801 ensure that the recipient has a copy of the transportation plan and understands the secure means of
802 onward movement of the classified material to its final destination, consistent with the approved
803 transportation plan. A freight forwarder or other transportation agent shall not be designated as a
804 DGR. Such entities merely facilitate the shipment of the material and are subject to U.S.
805 jurisdiction.

806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854

c. A military or commercial port of embarkation (POE) that is a recognized point of departure from the U.S. for on-loading aboard a ship, aircraft, or other carrier which is owned, controlled by, or registered to the recipient government. In such case, the transportation plan shall provide for U.S.-controlled shipment to the U.S. transshipment point and the identification of a cleared storage facility, U.S. Government or commercial, at or near the POE. The transportation plan shall identify the person who is to assume security oversight and control of the material while it is aboard the carrier. A DoD DGR or other designated U.S. Government official authorized to transfer custody shall supervise or observe the on loading of the classified material being transferred unless physical custody and security responsibility for the material is assumed by the recipient government's DGR prior to loading. In the event that transfer of physical and security custody cannot be accomplished promptly, the DoD official shall ensure that the classified material is either returned to a secure storage facility of the U.S. shipper, segregated and placed under constant surveillance of a duly cleared U.S. security force at the POE, or held in a secure storage facility designated in the transportation plan.

d. A cleared freight forwarder facility identified by the recipient government in the transportation plan as its transfer agent. Unless the recipient government DGR is present to accept delivery of the classified material and receipt for it, to include acceptance of security responsibility on behalf of the recipient government, the DoD DGR shall maintain oversight until the recipient government DGR signs for and accepts such responsibility. The freight forwarder is a transfer agent and shall not be the recipient government's DGR.

6. DELIVERY OUTSIDE THE UNITED STATES

a. Within the Recipient Country. Classified material to be delivered to a foreign government within the recipient country shall be delivered on arrival in the recipient country to a U.S. Government representative who shall arrange for its transfer to a DGR or other recipient government representative identified in the transportation plan. If a U.S. Government official authorized to accomplish the transfer of custody escorts the shipment, the material may be delivered directly to the recipient government's DGR or other recipient government representative upon arrival.

b. In a Third Country. Classified material to be delivered to a foreign government representative within a third country shall be delivered to an agency or installation of the U.S., or of the recipient government, that has extraterritorial status or otherwise is exempt from the jurisdiction of the third country. Unless a U.S. Government official authorized to accomplish the transfer of custody escorts the material, a U.S. Government official shall be designated locally to receive the shipment upon arrival and deliver it to a DGR or other recipient government representative identified in the transportation plan.

7. USE OF INTERNATIONAL CARRIERS. Transfers of classified material to locations outside the U.S. shall be made only via ships, aircraft, or other carriers as specified in Enclosure 4 of this Volume.

8. ESCORTS. Escorts are required aboard the carrier when transfers to a foreign government are

855 to occur outside the U.S. Escorts shall possess personnel security clearances of at least the same
856 classification level as the material to be transferred. The escorts shall be provided by the
857 implementing agency for FMS cases or by the U.S. cleared contractor for direct commercial sales,
858 unless:

859
860 a. The material is shipped by U.S. military carrier and the crew assumes control of the
861 material.

862
863 b. The recipient government DGR has signed for the consignment, a recipient-government
864 military carrier or carrier owned by or registered to the recipient government is used, and the
865 recipient government provides the cleared escort.

866
867 c. The exception authorized in paragraph 4.j. of Enclosure 4 is used and the conditions of that
868 paragraph are met.

869
870
871 9. RETURN FOR REPAIR, MODIFICATION, OR MAINTENANCE. Foreign governments may
872 return classified material for repair, modification, or maintenance. The requirements for return
873 shipment shall be specified in the LOA for FMS and in the security requirements section of a direct
874 commercial sales contract. The transfer procedures shall be in the original transportation plan and
875 shall include the same details on transportation channels, routes, transfer points, and identity of
876 responsible officials as specified for the original transfer.

877
878
879 10. TRANSPORTATION PLAN. The transportation plan required by paragraph 1.e. of this
880 appendix shall, at a minimum, include:

881
882 a. The purpose of the plan (i.e., FMS or direct commercial sale, with FMS case designator or
883 commercial contract identification), purchasing government, and date.

884
885 b. A description of the material to be shipped, identification of the associated FMS case or
886 contract line item(s), munitions list category, and classification.

887
888 c. A description of packaging requirements, seals, and storage requirements during shipment.

889
890 d. Identification, by name, title, organization of the DGRs, security and transportation officials
891 who will arrange the transfer of, sign receipts for, and assume security responsibility for the freight
892 during the transfer process. Mailing addresses, telephone numbers, fax numbers, and e-mail
893 addresses must be listed for each government's representatives.

894
895 e. Identification and specific location(s) of the delivery points, transfer points, and/or
896 processing points and description of the security arrangements for the material while located at each
897 point; if transfers will occur between carriers, explain the process, including the identification of
898 persons who will be involved.

899
900 f. Identification of commercial entities that will be involved in the shipping process (e.g.,
901 carriers and freight forwarders or transportation agents), the extent of their involvement, and their
902 clearance. Include names, addresses, telephone and fax numbers, e-mail addresses, and points of
903 contact.

904

905 g. A description of each segment of the route to be taken and, if applicable, security
906 arrangements for overnight stops or delays.

907

908 h. Arrangements for dealing with port and carrier security, immigration, and customs officials.
909 Identify personnel from each who have been consulted (and an alternate), and their telephone and
910 fax numbers, and e-mail addresses.

911

912 i. Names of escorts (and who they represent) or other responsible officials (e.g., Captain or
913 crew chief) to be used, including their government identification, passport numbers, security
914 clearances, and details concerning their responsibilities. Describe procedures for their accessibility
915 to the material while in storage. If the shipment will occur on a recurring basis, the shipper shall
916 provide an updated list of escorts with their identifying data prior to each shipment in accordance
917 with provisions of the approved plan.

918

919 j. A description of emergency procedures, and who is responsible for actions that must be
920 taken in the event of an emergency (e.g., unexpected stop anywhere along the route). Identify
921 individuals by name, and provide their organization, telephone and fax numbers, and e-mail
922 addresses.

923

924 k. Procedures for loading and securing the material.

925

926 l. Procedures for unloading the material and dealing with government port security, customs,
927 and immigration officials.

928

929 m. Identification, by name and personal identification, of the person who will ultimately sign
930 for and assume final control of the material for the recipient government.

931

932 n. A requirement for the recipient government to examine shipping documents upon receiving
933 classified material in its own territory and notify the DoD Component responsible for security of
934 the classified material if the material has been transferred in route to any carrier not authorized by
935 the transportation plan.

936

937 o. A requirement for the recipient government to inform the DoD Component responsible for
938 the security of the classified material promptly and fully of any known or suspected compromise of
939 the classified material.

940

941 p. Specific, detailed arrangements for return shipments for repair, overhaul, modification, or
942 maintenance (see section 9 of this appendix).

ENCLOSURE 5

SECURITY EDUCATION AND TRAINING

1. REQUIREMENT. The Heads of the DoD Components shall ensure that their personnel receive security education and training that:

- a. Provides necessary knowledge and information to enable quality performance of security functions.
- b. Promotes understanding of DoD Information Security Program policies and requirements and their importance to national security and national interests.
- c. Instills and maintains continuing awareness of security requirements.
- d. Assists in promoting a high degree of motivation to support program goals.
- e. ***(Added)(DAF) The commander or director will ensure all assigned DAF personnel performing security duties receive the appropriate security education and training, consistent with this Manual. (T-1).**

2. SECURITY EDUCATION AND TRAINING RESOURCES

- a. Security education and training may be accomplished by establishing programs within the DoD Component, using external resources such as the DCSA Academy, or a combination of the two.
- b. DoD Components may, if desired, combine into one overall program the education and training requirements of this enclosure and those for CUI specified in DoDI 5200.48.

3. INITIAL ORIENTATION. All personnel in the organization, including DoD civilians, military members, and on-site support contractors shall receive an initial orientation to the DoD Information Security Program.

- a. This initial orientation is intended to:
 - (1) Define classified information and CUI and explain the importance of protecting such information.
 - (2) Produce a basic understanding of security policies and principles.
 - (3) Notify personnel of their responsibilities within the security program, and inform them of the administrative, civil, and/or criminal sanctions that can be applied when appropriate.
 - (4) Provide individuals enough information to ensure the proper protection of classified

992 information and CUI in their possession, including actions to be taken if such information is
993 discovered unsecured, a security vulnerability is noted, or a person has been seeking unauthorized
994 access to such information.

995
996 (5) Inform personnel of the need for review of ALL unclassified DoD information prior to
997 its release to the public.

998
999 b. Security educators shall also consider including in the initial orientation identification of
1000 the DoD Component senior agency official and activity security management personnel, a
1001 description of their responsibilities, and whether they are involved in the protection of classified or
1002 controlled unclassified information. If not included in the initial orientation, such information must
1003 be included in the training required by paragraph 3.c. of this section.

1004
1005 c. In addition to the requirements in paragraphs 3.a. and 3.b. of this section, upon initial access
1006 to classified information, all personnel shall receive training on security policies and principles and
1007 derivative classification practices, including:

1008
1009 (1) The definition of classified information, the levels of classified information, and the
1010 damage criteria associated with each level.

1011
1012 (2) The responsibilities of DoD personnel who create or handle classified information,
1013 including:

1014
1015 (a) The requirements for controlling access to classified information, including:

1016
1017 1. The general conditions for and restrictions on access to classified information.

1018
1019 2. The steps an individual shall take when he or she is asked to verify classified
1020 information disclosed through unofficial open sources (e.g., news media, periodicals, and public
1021 websites).

1022
1023 (b) The policies and procedures for safeguarding classified information, including:

1024
1025 1. The proper methods and procedures for using, storing, reproducing,
1026 transmitting, disseminating, and destroying classified information.

1027
1028 2. The steps an individual shall take to safeguard classified information during
1029 an emergency evacuation situation.

1030
1031 3. The steps an individual shall take when he or she believes classified
1032 information has not been, or is not being, properly protected.

1033
1034 (c) The accountability of derivative classifiers for the accuracy of their work.

1035
1036 (3) An explanation that derivative classification is extracting, paraphrasing, or restating
1037 classified information based on a security classification guide, one or more source documents, or
1038 both.

1039
1040 (4) The authorized types of sources that can be used for derivative classification and

1041 where to obtain them, including:

1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089

(a) An explanation that a security classification guide:

1. Is precise, comprehensive guidance regarding specific program, system, operation or weapon system elements of information to be classified, including classification levels, reasons for classification, and the duration of classification.

2. Is approved and signed by the cognizant OCA.

3. Is an authoritative source for derivative classification.

4. Ensures consistent application of classification to the same information.

(b) How to use a security classification guide or other derivative source.

(c) How and where to obtain classification guidance currently available for a specific area of expertise, including:

1. The security manager and/or the program or project office.

2. The Defense Technical Information Center, at <https://discover.dtic.mil/> (registration required).

3. In the case of a military operation and the creation or execution of plans and orders thereto, the higher headquarters office that mandated or directed the operation or mission.

(5) The proper and complete classification markings to be used for classified information, and how those markings are to be applied, including:

(a) The importance of properly applying the authorized classification markings and the need to avoid over-classification.

(b) How to document the level of classification, duration of classification and the source(s) of classified information included in the material (e.g., document, e-mail, briefing, video) being created or generated.

(c) How to observe and respect the original classification decision(s).

(d) How to maintain lists of sources when multiple sources of classification are used.

(e) How to determine the duration of classification.

(f) How to properly use control markings to limit or expand distribution, including foreign disclosure and release markings (e.g., “REL TO” (releasable to), “NOFORN” (not releasable to foreign nationals) and DISPLAY ONLY).

(g) How to challenge classification decisions.

1090 (h) How to downgrade or declassify information as an authorized holder of
1091 information in accordance with the direction of the cognizant OCA or classification guide.
1092

1093 (i) How to mark and share “working papers” and other drafts, including the
1094 requirements for such markings.
1095

1096 (6) The definition of a security incident, a violation and a compromise of classified
1097 information, examples of each, and an explanation of the criminal, civil, and administrative
1098 sanctions that may be taken against an individual who fails to comply with program requirements
1099 or to protect classified information from unauthorized disclosure.
1100

1101 (7) The policies and procedures for sharing classified information with state, local, tribal,
1102 and private sector officials and with foreign governments and international organizations, including
1103 the markings that designate information as qualifying for sharing, if appropriate for the activity’s
1104 mission or function.
1105

1106 (8) The policies and procedures for the marking, safeguarding, and accounting of NATO
1107 classified information.
1108

1109 d. In addition to the training specified by paragraphs 3.a through 3.c of this section and
1110 cybersecurity training required by DoDD 8570.01 (Reference (bh)), personnel who are authorized
1111 access to classified information systems shall receive training which specifically addresses:
1112

1113 (1) Proper use of information systems for creating, using, storing, processing, or
1114 transmitting classified information.
1115

1116 (2) The requirement for and application of markings, including portion markings, to
1117 information in electronic formats (e.g., documents, e-mail, briefings, web-based information,
1118 databases, spreadsheets).
1119

1120 (3) Marking, handling, storage, transportation, and destruction of classified computer
1121 media (e.g., CDs, DVDs, removable hard drives).
1122

1123 (4) Procedures to be followed when using classified removable data storage media.
1124

1125 (5) Procedures to be followed if an individual believes an unauthorized disclosure of
1126 classified data has occurred on an information system or network (typically called a “data spill”).
1127

1128 1129 4. SPECIAL TRAINING REQUIREMENTS 1130

1131 a. Individuals with specified duties in the Information Security Program, as identified in
1132 sections 5, 6 and 10 of this enclosure, shall be provided security education and training
1133 commensurate with job responsibilities and sufficient to permit effective performance of those
1134 duties. The education and training may be provided before, concurrent with, or not later than 6
1135 months following assuming those duties, unless otherwise specified.
1136

1137 b. Deployable organizations shall provide, prior to deployment, enhanced security training to
1138 meet the needs of the operational environment. Where appropriate, this pre-deployment training

1139 shall specifically address security requirements associated with information sharing (e.g., release of
1140 information to state, local, tribal, or coalition partners; use and handling of FGI) and shall provide
1141 training on the classification markings that are to be applied in these situations and that designate
1142 information as qualifying for sharing.

1143
1144 c. Additional security education and training may be required for personnel who:

1145
1146 (1) Travel to foreign countries where special concerns about possible exploitation exist or
1147 attend professional meetings or conferences where foreign attendance is likely.

1148
1149 (2) Escort, hand-carry or serve as a courier for classified material.

1150
1151 (3) Are authorized access to classified information requiring special control or
1152 safeguarding measures.

1153
1154 (4) Are involved with international programs.

1155
1156 (5) Are involved with acquisition programs subject to Reference (ae).

1157
1158 (6) Are involved with FGI, or work in coalition or bilateral environments, or in offices,
1159 activities, or organizations hosting foreign exchange officers.

1160
1161 (7) Submit information to OCAs for original classification decisions and therefore need
1162 additional knowledge of the original classification decision process.

1163
1164
1165 5. OCA TRAINING. Training for newly appointed OCAs shall be provided prior to exercise of
1166 the authority and each OCA shall receive training annually thereafter as required in paragraph
1167 7.b. of this enclosure. The OCA shall certify in writing that the training has been received.
1168 Personnel preparing recommendations for original classification to OCAs will receive the same
1169 training. The training shall address OCA responsibilities and classification principles, proper
1170 safeguarding of classified information, and the criminal, civil, and administrative sanctions that
1171 may be brought against an individual. At a minimum, the training shall address:

1172
1173 a. General requirements, including:

1174
1175 (1) The difference between original and derivative classification.

1176
1177 (2) Persons who can classify information originally.

1178
1179 (a) OCA is assigned to a position, not a person and, except as authorized by Enclosure
1180 4 of Volume 1 of this Manual, may not be further delegated.

1181
1182 (b) Only individuals carrying out a unique mission with responsibility in one of the
1183 subject areas prescribed by section 1.4 of Reference (d) may be designated an OCA.

1184
1185 (c) Deputies, vice commanders, chiefs of staff, and similar immediate subordinates of
1186 an OCA are empowered to exercise OCA when they have been officially designated to assume the
1187 duty position of the OCA in an acting capacity during the OCA's absence and have certified in

1188 writing that they have received required OCA training.

1189
1190 (3) The requirement to certify, in writing, before initially exercising OCA authority and
1191 annually thereafter, that training has been received.

1192
1193 (4) The prohibitions and limitations on classifying information, as stated in sections 1 and
1194 2 of Enclosure 4 of Volume 1 of this Manual, and the need to avoid over classification.

1195
1196 (5) ***(Added)(DAF) Personnel who assist in developing SCGs must take the same**
1197 **training, annually, as the OCA. (T-1). Training must be recorded in the approved system of**
1198 **record. (T-1).**

1199
1200 b. The responsibility and discretion the OCA has in classifying information.

1201
1202 (1) OCAs must be aware that their decisions to classify information have a substantial
1203 impact on the operations of the Department and on national security. Others who work with the
1204 information use these original decisions to make proper derivative classification decisions and to
1205 assure that the information is properly protected from unauthorized disclosure.

1206
1207 (2) OCAs are accountable to the Secretary of Defense for their classification decisions.

1208
1209 (3) OCAs shall exercise a substantial degree of autonomy in operations or mission.
1210 Information warranting original classification must be developed in the normal course of actions or
1211 activity.

1212
1213 c. The classification principles and process specified in section 6, Enclosure 4 of Volume 1
1214 of this Manual.

1215
1216 (1) Original classification requires identification of specific elements of information
1217 which could adversely affect the national security if compromised. In addition to consideration of
1218 harm to the national security, OCAs must weigh the advantages and disadvantages of classifying
1219 each element and should consider, when applicable:

1220
1221 (a) Degree of intended or anticipated dissemination or use.

1222
1223 (b) Net national advantage.

1224
1225 (c) Lead time advantage for operational or technological use.

1226
1227 (d) Cost in terms of time, money, and personnel.

1228
1229 (e) Impact on attaining the program objective.

1230
1231 (f) State of the art and public knowledge of the U.S. interest.

1232
1233 (g) Appearance in the public domain, inadvertent disclosure or other compromise.

1234
1235 (h) Basic scientific research data or unusually significant scientific findings.

1236

1237 (i) Association or compilation of information or data.
1238

1239 (2) Information is classified either because its unauthorized disclosure could reasonably be
1240 expected to cause identifiable or discernable damage to national security or because it may reveal
1241 such information when associated with other information. If information is classified in
1242 compilation with other information, a clear explanation of rationale must be provided (see section
1243 12 of Enclosure 3 of Volume 2).
1244

1245 (3) OCAs shall ensure that a review for possible declassification is conducted
1246 expeditiously in the event of compromise, that damage assessments are conducted as necessary,
1247 and that formal challenges to classification, classification conflicts, and requests for classification
1248 determinations from individuals who are not OCAs are addressed as required by this Manual.
1249

1250 d. The procedures that must be followed when making and communicating original
1251 classification decisions.
1252

1253 (1) The required markings that must appear on classified information as specified in
1254 Volume 2, Enclosure 3 of this Manual.
1255

1256 (2) The process for determining duration of classification.
1257

1258 (a) Information shall be assigned a date or event for declassification that is 25 years or
1259 less from the date of origination, except for information that is clearly and demonstrably expected
1260 to reveal the identity of a confidential human source or a human intelligence source or key design
1261 concepts of weapons of mass destruction.
1262

1263 (b) Information in records with permanent historic value may be classified for longer
1264 than 25 years only if the Interagency Security Classification Appeals Panel (ISCAP) has been
1265 notified of such a date in accordance with the procedures in section 13, Enclosure 5 of Volume 1 of
1266 this Manual. The ISCAP decisions will be codified in a classification or declassification guide.
1267

1268 (3) The general standards and procedures for changes in classification (downgrade,
1269 upgrade, declassify) and the general requirements for automatic and systematic declassification and
1270 mandatory reviews for declassification.
1271

1272 (a) An OCA should organize the classification process around time and event-phased
1273 downgrading and declassification events to the maximum extent possible.
1274

1275 (b) An OCA may change the level of classification of information under their
1276 jurisdiction (downgrade, upgrade, declassify) as specified in section 7, Enclosure 4 of Volume 1 of
1277 this Manual.
1278

1279 (c) Classification may change at each phase of an operation, research and
1280 development cycle, or acquisition, as determined by the OCA with responsibility over the
1281 information.
1282

1283 (4) The requirements and standards for creating, issuing, and maintaining security
1284 classification guidance, including classification and declassification guides, as identified in section
1285 8, Enclosure 4 of Volume 1 of this Manual.

1286
1287 e. The proper safeguarding protections to apply when using, storing, reproducing,
1288 transmitting, disseminating, and destroying classified information.

1289
1290 f. The criminal, civil, and administrative sanctions that may be brought against an individual
1291 who fails to classify information properly or to protect classified information from unauthorized
1292 disclosure.

1293
1294
1295 6. DECLASSIFICATION AUTHORITY TRAINING. The security education and training
1296 provided declassification authorities other than original classifiers shall, at a minimum, address:

1297
1298 a. The standards, methods, and procedures for declassifying information pursuant to
1299 References (d) and (f) and this Manual.

1300
1301 b. The standards for creating, maintaining, and using declassification guides.

1302
1303 c. The information contained in the DoD Component's declassification plan.

1304
1305 d. The DoD Component's responsibilities for establishing and maintaining a declassification
1306 database.

1307
1308 e. The referral process and requirements.

1309
1310
1311 7. ANNUAL REFRESHER TRAINING

1312
1313 a. At a minimum, all DoD civilians, military members, and on-site support contractors with
1314 access to classified information shall receive annual refresher training that reinforces the policies,
1315 principle, and procedures covered in their initial and specialized training. Refresher training shall
1316 also address the threat and the techniques foreign intelligence activities use while attempting to
1317 obtain classified DoD information, and advise personnel of penalties for engaging in espionage
1318 activities and other unauthorized disclosures. Refresher training shall also address relevant
1319 changes in information security policy or procedures and issues or concerns identified during DoD
1320 Component self-inspections. Information system users shall additionally complete an annual
1321 cybersecurity awareness refresher, as required by Reference (bf).

1322
1323 b. Each OCA shall receive annual training as specified in section 5 of this enclosure. The
1324 OCA shall certify receipt of the training in writing. OCAs who do not receive the specified
1325 training at least once within a calendar year shall have their classification authority suspended by
1326 the DoD Component Head or the senior agency official who delegated the authority until the
1327 training has taken place, unless a waiver is granted in accordance with paragraph 7.f of this section.

1328
1329 c. Derivative classifiers (i.e., those who create new documents, including e-mails, based on
1330 existing classification guidance) shall receive training in derivative classification as required by
1331 paragraph 3.c. of this enclosure, with an emphasis on avoiding over-classification, at least once
1332 every year. Training may, at the DoD Component's discretion, be included in the training required
1333 by paragraph 7.a. of this section. Derivative classifiers who do not receive training at least once
1334 every year shall not be authorized or allowed to derivatively classify information until they have

1335 received training, unless a waiver is granted in accordance with paragraph 7.f of this section.

1336
1337 d. Declassification authorities shall receive training as required by section 6 of this enclosure
1338 at least once every 2 years.

1339
1340 e. DoD Components shall track training required by paragraphs 7.b and 7.c of this section and
1341 take appropriate action to suspend OCA authority in accordance with paragraph 7.b or disallow
1342 derivative classification in accordance with paragraph 7.c if the training is not accomplished as
1343 required.

1344
1345 f. A waiver to the training requirement in paragraphs 7.b or 7.c of this section may be granted
1346 by the DoD Component Head, the Deputy Component Head, or senior agency official if an
1347 individual is unable to receive required training due to unavoidable circumstances. Whenever a
1348 waiver is granted, the individual shall receive the required training as soon as practicable.

1349
1350 g. ***(Added)(DAF) In accordance with reference (cn) (or successor policy), all DoD**
1351 **personnel who process classified information shall complete derivative classification training,**
1352 **on an annual basis. (T-0). Additionally, DAF personnel that require a Secret Internet**
1353 **Protocol Router Network (SIPRNet) account must take the aforementioned derivative**
1354 **classification training prior to receiving an account and annually thereafter. (T-0).**

1355
1356
1357 8. CONTINUING SECURITY EDUCATION AND TRAINING. Security education and training
1358 shall be continuous, rather than aperiodic. Periodic briefings, training sessions, and other formal
1359 presentations shall be supplemented with other information and promotional efforts to ensure that
1360 continuous awareness and performance quality is maintained. The use of job performance aids and
1361 other substitutes for formal training is encouraged when they are determined to be the most
1362 effective means of achieving program goals. The circulation of directives or similar material on a
1363 read-and-initial basis shall not be considered as the sole means of fulfilling any of the specific
1364 requirements of this enclosure.

1365
1366
1367 9. TERMINATION BRIEFING. The DoD Components shall establish procedures to ensure that
1368 cleared employees who leave the organization or whose clearance is terminated receive a
1369 termination briefing, in accordance with paragraph C9.2.5 of Reference (l). The briefing shall:

1370
1371 a. Emphasize their continued responsibility to protect classified and controlled unclassified
1372 information to which they have had access.

1373
1374 b. Provide instructions for reporting any unauthorized attempt to gain access to such
1375 information.

1376
1377 c. Advise the individuals of the prohibitions against retaining classified and controlled
1378 unclassified material when leaving the organization.

1379
1380 d. Identify the requirement that retired personnel, former DoD employees, and non-active duty
1381 members of the Reserve Components must submit writings and other materials intended for public
1382 release to the DoD security review process as specified by Reference (k).

1384 e. Remind them of the potential civil and criminal penalties for failure to fulfill their
1385 continuing security responsibilities.

1386
1387
1388 10. MANAGEMENT AND OVERSIGHT TRAINING. Individuals designated as security
1389 managers, classification management officers, security specialists, or any other personnel whose
1390 duties significantly involve managing and overseeing classified information shall receive training
1391 that meets the requirements of DoDI 3305.13 (Reference (bg)) and addresses:

- 1392 a. The original and derivative classification processes and the standards applicable to each.
1393
1394 b. The proper and complete classification markings to be applied to classified information,
1395
1396 c. The proper use of control markings to limit or expand distribution, including foreign
1397 disclosure and release markings (e.g., REL TO, NOFORN, and DISPLAY ONLY).
1398
1399 d. The authorities, methods, and processes for downgrading and declassifying information.
1400
1401 e. The methods for properly using, storing, reproducing, transmitting, disseminating, and
1402 destroying classified information.
1403
1404 f. The requirements for creating, maintaining, and issuing classification and declassification
1405 guides.
1406
1407 g. The requirements for controlling access to classified information.
1408
1409 h. The procedures for investigating and reporting instances of actual or potential
1410 compromise of classified information, including when in electronic form, and the penalties that
1411 may be associated with violating established security policies and procedures.
1412
1413 i. The requirements for creating, maintaining, and terminating SAPs, and the mechanisms for
1414 monitoring such programs.
1415
1416 j. The procedures for the secure use of information systems and networks that use, process,
1417 store, reproduce, or transmit classified information, and requirements for their certification and
1418 accreditation.
1419
1420 k. The provisions for automatic declassification and the need for systematic and mandatory
1421 reviews for declassification, and the DoD Component procedures for accomplishing each.
1422
1423 l. The requirements for overseeing the Information Security Program, including self-
1424 inspections.
1425
1426 m. ***(Added)(DAF) For activity security manager's, completion of any one of the below
1427 curriculums, courses and/or certifications, located on the Center for Development of Security
1428 Excellence website, will satisfy this requirement. (T-1).**

1429
1430
1431 (1) ***(Added)(DAF) Air Force Security Manager Program curriculum (GS100.CU);**
1432

1433 (2) ***(Added)(DAF) Instructor-led DoD Security Specialist course (GS101.01); or,**

1434
1435 (3) ***(Added)(DAF) If conferral of the Security Fundamentals Professional**
1436 **Certification, under the DoD Security Professional Education Development program (see**
1437 **reference (bg)) can be confirmed prior to appointment, the individual does not need to**
1438 **complete 10.m.(1) or 10.m.(2) (above).**

1439
1440 (a) ***(Added)(DAF) Civilian or military personnel serving as an assistant security**
1441 **manager will train to the same standard as the activity security manager. (T-1). Training**
1442 **must be completed within six months of assuming duties and commensurate to the level and**
1443 **complexity of the security program. (T-1).**

1444
1445 (b) ***(Added)(DAF) Civilian, military or on-site contractor personnel serving as a**
1446 **security assistant will be trained on the specific administrative actions being undertaken. (T-**
1447 **1).**

1448
1449 (c) ***(Added)(DAF) In addition to the above training requirements, the IP office**
1450 **will work with the commander or director to develop a more specified security training**
1451 **program, corresponding with job responsibilities and tailored around the command's**
1452 **mission or other unique operational requirements. (T-1).**

1453
1454
1455 11. PROGRAM OVERSIGHT. The Heads of the DoD Components shall ensure that security
1456 education and training are appropriately evaluated during self-inspections and other oversight
1457 activities. This evaluation shall include assessing the quality and effectiveness of the efforts, as
1458 well as ensuring appropriate coverage of the target populations. The Heads of the DoD
1459 Components shall require maintaining records of education and training offered and employee
1460 participation, as they deem necessary to permit effective oversight.

ENCLOSURE 6SECURITY INCIDENTS INVOLVING CLASSIFIED INFORMATION

1. INTRODUCTION. Protection of classified information is essential to maintaining security and achieving mission success in DoD operational and warfighting environments. Prompt reporting of security incidents ensure that such incidents are properly investigated and the necessary actions are taken to negate or minimize the adverse effects of an actual loss or unauthorized disclosure of classified information and to preclude recurrence through an informed, properly tailored, and up-to-date security education and awareness program. In cases where compromise has been ruled out and there is no adverse effect on national security, a common sense approach to the early resolution of an incident at the lowest appropriate level is encouraged. All security incidents involving classified information shall involve a security inquiry, a security investigation, or both.

a. The terms associated with security incidents are formally defined in the Glossary, but to ensure common understanding, the following general characterizations are provided:

(1) Infraction. An infraction is a security incident involving failure to comply with requirements (i.e., the provisions of References (d) and (f), this Manual or other applicable security policy) which cannot reasonably be expected to, and does not, result in the loss, suspected compromise, or compromise of classified information. An infraction may be unintentional or inadvertent. While it does not constitute a security violation, if left uncorrected, can lead to security violations or compromises. It requires an inquiry to facilitate immediate corrective action but does not require an in-depth investigation.

(2) Violation. Violations are security incidents that indicate knowing, willful, and negligent for security regulations, and result in, or could be expected to result in, the loss or compromise of classified information. Security violations require an inquiry and/or investigation.

(a) Compromise. A compromise is a security incident (more specifically, a violation) in which there is an unauthorized disclosure of classified information (i.e., disclosure to a person(s) who does not have a valid clearance, authorized access, or a need to know).

(b) Loss. A loss occurs when classified information cannot be physically located or accounted for (e.g., classified information/equipment is discovered missing during an audit and cannot be immediately located).

(3) Inquiry. An inquiry is fact-finding and analysis conducted to determine whether or not there was a loss of classified information or whether or not unauthorized personnel had, or could have had, access to the information. The inquiry identifies the facts, characterizes the incident as an infraction or a violation, identifies if possible the cause(s) and person(s) responsible, reports corrective actions taken or to be taken, and makes recommendations as to the need for further corrective action or a more in-depth investigation. Inquiries, generally, are initiated and conducted at the lowest echelon possible within the DoD Component.

1510 (4) Investigation. An investigation is conducted for a security violation when the incident
1511 cannot be resolved via inquiry or for incidents where an in-depth and comprehensive examination
1512 of the matter is appropriate.

1513
1514 b. Certain practices dangerous to security, while not reportable as security incidents, have the
1515 potential to jeopardize the security of classified information and material if allowed to perpetuate.
1516 Examples of such practices are: placing a paper recycling box next to a classified copier or placing
1517 burn bags next to unclassified trash containers; stopping at a public establishment to conduct
1518 personal business while hand-carrying classified information; or failing to change security
1519 container combinations promptly when required. These practices, when identified, must be
1520 promptly addressed by security management and appropriate changes made, actions taken, or
1521 training provided, to ensure the security of classified information.

1522
1523 c. ***(Added)(DAF) Maintain security incident reports in accordance with AFRIMS,**
1524 **Table 31-04, Rule 13.00 (or subsequent revisions). (T-1).**

1525
1526
1527 2. CONSEQUENCES OF COMPROMISE. The compromise of classified information presents a
1528 threat to the national security and may damage intelligence or operational capabilities; lessen the
1529 DoD ability to protect critical information, technologies, and programs; or reduce the effectiveness
1530 of DoD management. Once a compromise is known to have occurred, the seriousness of damage to
1531 U.S. national security or the extent of the adverse effect on the national security must be
1532 determined and appropriate measures taken to negate or minimize the adverse effects. When
1533 possible, action shall also be taken to regain custody of documents or material that was
1534 compromised. In all cases, security management must take appropriate action to identify the source
1535 and reason for the suspected or actual compromise and take remedial action to prevent recurrence.

1536 1537 1538 3. REPORTING AND NOTIFICATIONS

1539
1540 a. Anyone finding classified information out of proper control shall, if possible, take custody
1541 of and safeguard the material and immediately notify the appropriate security authorities. Secure
1542 communications should be used for notification whenever possible.

1543
1544 b. Every civilian employee and Active, Reserve, and National Guard Military member of the
1545 DoD, and every DoD contractor or employee of a contractor working with classified material, as
1546 provided by the terms of the contract, who becomes aware of the loss or potential compromise of
1547 classified information shall immediately report it to the head of his or her local activity and to the
1548 activity security manager.

1549
1550 c. If the person believes that the head of the activity or the security manager may have been
1551 involved in or responsible for the incident, he or she may report it to the security authorities at the
1552 next higher level of command or supervision. If circumstances of discovery make such notification
1553 impractical, the individual shall notify the commanding officer or security manager at the most
1554 readily available DoD facility or contact any DoD law enforcement, counterintelligence (CI), or
1555 Defense Criminal Investigative Organization (DCIO).

1556
1557 d. Security managers shall advise their chain of command of compromises occurring within
1558 their area of security responsibility or involving assigned personnel.

1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607

e. If the head of an activity or the activity security manager to whom an incident is initially reported does not have security cognizance over the incident, such official shall ensure that the incident is reported to the appropriate authority. The organization with security cognizance shall ensure that an inquiry and, when appropriate, investigation are conducted, as needed, consistent with the requirements of this enclosure and corrective action is taken as required.

f. Reporting confirmed security incidents to the Director of Security, USD(I&S), is necessary when the incidents have or may have significant consequences or the fact of the incident may become public. Such incidents shall be reported promptly through appropriate security channels by the DoD Component senior agency official. When appropriate, preliminary reports shall be provided, particularly when the fact of the incident may become public or attract media attention.

(1) The Director of Security, USD(I&S), shall be notified of:

(a) A violation involving espionage.

(b) An unauthorized disclosure of classified information in the public media. See section 7 of this enclosure for information required in the notification. Additional notification is not required for reference to or republication of a previously identified media disclosure.

(c) Any violation wherein properly classified information is knowingly, willfully, or negligently disclosed to unauthorized persons or information is classified or continues to be classified when that violation:

1. Is reported to the oversight committees of Congress;

2. May attract significant public attention;

3. Involves large amounts of classified information; or

4. Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

(d) Any violation wherein a SAP is knowingly, willfully, or negligently created or continued contrary to the requirements of Reference (ah), DoDI O-5205.11 (Reference (bh)), this Manual, and national policies.

(e) A security failure or compromise of classified information relating to any defense operation, system, or technology that is likely to cause significant harm or damage to U.S. national security interests, for which Congressional reporting may be required by section 2723 of title 10, U.S.C. (Reference (bi)).

(f) Other egregious security incident (as determined by the DoD Component SAO).

(2) Security incidents that do not meet the reporting criteria specified above shall be filed in a retrievable format by the DoD Component and shall be available for inspection or further analysis, review, and potential investigation.

1608

1609 (3) On behalf of the Secretary of Defense, the USD(I&S) shall notify Congress and the Director,
1610 ISOO, regarding specific cases or incidents as required by References (d) and (bk).

1611

1612 (4) The Director of Security, USD(I&S), shall coordinate with the Office of the DNI
1613 (ODNI) National Counterintelligence Executive (NCIX), as needed, to ensure notifications required
1614 by Intelligence Community Directive 701 (Reference (bj)) are made.

1615

1616 g. All DAF personnel who become aware of any possible security incident involving classified
1617 information, regardless of whether it did or could have resulted in an actual, potential or suspected
1618 loss or compromise of classified information shall immediately report it to their commander or
1619 director, supervisor, and security manager (T-1). Supervisors and security managers (or security
1620 assistant) shall report the security incident to their commander or director (T-1). The commander
1621 or director shall report the incident to the responsible IP office (T-1). The responsible IP office will
1622 assist the commander or director in determining if the incident warrants a formal inquiry (T-1).
1623 The responsible IP office will track and provide oversight of the security incident (T-1). If needed,
1624 document the process in the wing instruction.”

1625

1626

1627 4. CLASSIFICATION OF REPORTS

1628

1629 a. Security incident reports shall be classified according to the content of the report and at the
1630 level prescribed by the applicable program security classification guides. At a minimum, reports
1631 shall be marked as required by DoDI 5200.48, in order to provide appropriate protection for
1632 information regarding personnel involved and information that could facilitate unauthorized access
1633 to classified information. If the lost or compromised information is beyond the jurisdiction of the
1634 U.S. Government and cannot be recovered (e.g., media leak, public website posting, or loss in a
1635 foreign country), the report and location of the compromise (e.g., geographic location of
1636 unrecoverable equipment) shall be classified commensurate with the classification level of the
1637 compromised material to prevent further unauthorized disclosure.

1638

1639 b. If a report is to be disseminated outside the DoD (e.g., to another Federal agency), the face
1640 of the document shall bear an expanded marking, as specified in DoDI 5200.48.

1641

1642 c. Reports, whether classified or unclassified, disclosing technical data shall be marked with
1643 the appropriate distribution statement as described in DoDD 5230.24 (Reference (bl)) or associated
1644 with the information involved in the incident.

1645

1646

1647 5. SPECIAL CIRCUMSTANCES. Certain types of classified information or specific
1648 circumstances require unique handling or consideration of additional reporting requirements as
1649 specified in paragraphs 5.a through 5.o.

1650

1651 a. Security Incidents Involving Deliberate Compromise, a Foreign Intelligence Service or a
1652 Terrorist Organization

1653

1654 (1) Any incident in which deliberate compromise of classified information or involvement
1655 of a foreign intelligence service, international terrorist group, or organization is suspected shall be
1656 reported immediately to the cognizant Defense CI component, in accordance with DoDD 5240.06

1657 (Reference (bm)). Security officials shall not initiate or continue an inquiry or investigation of the
1658 incident unless it is fully coordinated with the cognizant Defense CI component.

1659
1660 **(2) (Added)(DAF) In accordance with AFI 71-101, *Criminal Investigations Program*,**
1661 **DAF personnel shall immediately report these types of security incidents to the Air Force**
1662 **Office of Investigations (OSI). (T-1). Security officials shall not initiate or continue an**
1663 **inquiry or investigation of the incident unless it is fully coordinated and concurred by the OSI**
1664 **detachment commander or special agent-in-charge. (T-1).**

1665
1666 b. Security Incidents Involving Apparent Violations of Criminal Law. Any incident in which
1667 an apparent violation of criminal law is suspected, but which is reasonably not believed to be
1668 espionage or involving matters described in paragraph 5.a of this section, shall be reported
1669 immediately to the local DCIO. If that organization accepts jurisdiction and initiates action,
1670 coordinate with them prior to taking any further action on the security inquiry or investigation so as
1671 not to jeopardize the integrity of either investigation.

1672
1673 c. Security Incidents Involving COMSEC or Cryptologic Information. Actual or potential
1674 compromises involving cryptographic information shall be handled according to NSTISSI 4003
1675 (Reference (bp)).

1676
1677 d. Security Incidents Involving SCI. Actual or potential compromises involving SCI shall be
1678 reported to the activity SSO and handled in accordance with References (i) and (bj).

1679
1680 (1) Incidents involving SCI that meet the criteria in paragraph 3.f of this enclosure shall
1681 also be reported to the Director of Security, USD(I&S).

1682
1683 (2) If a DoD Component believes a disclosure may contain classified SCI information
1684 under the control of another Intelligence Community agency, the DoD Component shall notify
1685 NCIX. NCIX shall coordinate notification to the affected agency.

1686
1687 e. Security Incidents Involving RD and/or FRD. In accordance with the provisions of section
1688 3161 of Public Law 105-261 (Reference (bo)), and its implementing plan, the Secretary of Energy
1689 must report to Congress inadvertent disclosure of RD or FRD occurring pursuant to automatic
1690 declassification processes. Components shall notify the DOE, as necessary, and provide a copy of
1691 the notification to the Deputy Assistant Secretary of Defense for Nuclear Matters and the Director
1692 of Security, USD(I&S).

1693
1694 f. Security Incidents Involving IT. Actual or potential compromises of classified information
1695 involving IT, automated information systems, or computer systems, terminals, or equipment shall
1696 be reported, in accordance with Reference (v), through appropriate channels by the IA manager
1697 (IAM) to the activity security manager. Inquiries into and resolution of incidents involving
1698 compromise of classified information resident on computers or in IT systems require coordination
1699 with and assistance from the local IA officials, but prompt resolution remains the responsibility of
1700 the activity security manager. See Enclosure 7 for additional guidance on handling of classified
1701 data spills.

1702
1703 g. Security Incidents Involving FGI or NATO Information. Actual or potential compromises
1704 involving FGI or NATO information shall also be reported promptly by the DoD Component senior
1705 agency official to the USD(P), who serves as the DSA. The Director, International Security

1706 Programs, Defense Technology Security Administration, USD(P), shall be responsible, on behalf of
1707 the DSA, for notifying and coordinating with NATO or the foreign government, as appropriate.
1708

1709 h. Security Incidents Involving Classified U.S. Information Provided to Foreign Governments.

1710 Actual or potential compromises of U.S. classified information held by foreign governments shall
1711 be reported to the originating DoD Component, the OCA, the Director of Security, USD(I&S), and
1712 the Director, International Security Programs, Defense Technology Security Administration,
1713 USD(P).
1714

1715 i. Security Incidents Involving SAPs. Actual or potential compromises involving DoD SAPs,
1716 or results of inquiries and/or investigations that indicate that weaknesses or vulnerabilities in
1717 established SAP policy and/or procedures contributed to an actual or potential compromise, shall be
1718 reported by the DoD Component SAP program office to the DoD SAP Central Office, which shall
1719 report to the Director of Security, USD(I&S).
1720

1721 j. Security Incidents Involving Improper Transfer of Classified Information. Any activity that
1722 receives classified information that has been improperly handled, addressed, packaged, transmitted,
1723 or transported shall make a determination as to whether the information has been subjected to
1724 compromise. If the activity determines that the classified information has been subjected to
1725 compromise, the receiving activity shall immediately notify the sending activity, which shall be
1726 responsible for initiating an inquiry or investigation, as appropriate. The receiving activity shall
1727 share information generated regarding the incident with the sending activity. The sending activity
1728 is responsible for required notifications (e.g., to the OCA). Classified information shall be
1729 considered as having been subjected to compromise if it has been handled through foreign postal
1730 systems, its shipping container has been damaged to an extent that the contents are exposed, or it
1731 has been transmitted (e.g., telephone, facsimile, message, e-mail, computer or data links) over
1732 communications circuits that are not approved for transmission of classified information. If the
1733 receiving activity determines that classified information was not in fact compromised, but was
1734 nevertheless improperly prepared or transferred, the receiving activity shall report the discrepancy
1735 to the sending activity.
1736

1737 k. Security Incidents Involving On-Site Contractors. Security incidents, including any
1738 inquiries or investigations required, involving on-site contractors shall be handled in accordance
1739 with paragraph C1.1.9 of Reference (az). As specified by paragraph C1.1.9 of Reference (az) and
1740 paragraph 6-105c of Reference (w), host activity security rules and procedures apply. Disciplinary
1741 action and sanctions are the responsibility of the contractor's company unless specific contract
1742 provisions address such actions. Activity security managers shall furnish the results of inquiries to
1743 the company, with a copy to DCSA, in order to facilitate such action. Specified U.S. Government
1744 officials retain the ability, when appropriate and in accordance with the authorities and
1745 requirements of Reference (az), to deny access to classified information, to revoke or suspend
1746 security clearances, and to take certain other administrative actions, such as to deny an individual
1747 continued access to the facility.
1748

1749 l. Security Incidents Involving Critical Program Information (CPI). Upon learning that
1750 classified CPI or CPI related to classified contracts may have been or was actually compromised,
1751 security officials shall inform the program manager of record and the cognizant Defense CI
1752 component pursuant to DoDD 5240.02 (Reference (bp)). The specific CPI involved in the incident
1753 should be identified in inquiry and investigation reports. Classify reports as required by the
1754 applicable program security classification guide(s).

1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803

m. Security Incidents Involving ACCM-Protected Information. Security officials shall refer to section 18 of Enclosure 2 of this Volume for additional guidance on security incidents involving ACCM-protected information as well as safeguarding and handling of ACCM-protected information.

n. Absence without Authorization. When an individual who has had access to classified information is absent without authorization, the head of the activity or activity security manager shall determine if there are indications of activities, behavior, or associations that could indicate classified information may be at risk. If so, the supporting Defense CI component shall be notified in accordance with Reference (bp). The scope and depth of the inquiry shall depend on the length of absence and the sensitivity of the classified information involved. Missing personnel authorized SCI access shall be reported in accordance with Reference (i).

o. Coordination with Legal Counsel and the Department of Justice (DoJ). Whenever formal action, beyond adjudication of a finding of a security violation and assignment of reprimand or disciplinary action at the activity level is contemplated against any person believed responsible for the unauthorized disclosure of classified information, DoD Component officials shall coordinate with servicing legal counsel. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, Component officials shall use established procedures and channels to ensure coordination with the legal counsel of the DoD Component or Federal agency where the individual is assigned or employed and the DoJ.

6. SECURITY INQUIRIES AND INVESTIGATIONS

a. Requirement. All known or suspected instances of unauthorized disclosure of classified information shall be promptly addressed by the cognizant DoD Component to decide the nature and circumstances of the disclosure and the extent of damage to national security, and appropriate corrective action shall be taken. See Appendix 1 to this enclosure for a sample, optional format for use in documenting actions. Reports of inquiries and investigations, at a minimum, shall be designated and marked as required by DoDI 5200.48.

b. Coordination with Criminal Investigative Organization or Defense CI Component. When information suggestive of a criminal or CI nature is discovered, all actions associated with the inquiry or investigation shall cease pending coordination with the cognizant DCIO or Defense CI component. If the DCIO or Defense CI component accepts jurisdiction, the inquiry or investigation shall not be resumed without agreement of the cognizant criminal investigative organization or CI component. All relevant information shall be released with an annotation in the report that the matter was referred to the specific DCIO or Defense CI component. Notify the OCA, originator, and others as appropriate, after coordination with the DCIO or Defense CI component. If the DCIO or Defense CI component declines jurisdiction, the security inquiry or investigation shall continue. Annotate the report appropriately and include the identity of the official who made the declination decision and his or her organization.

c. Coordination with OCA

(1) If the inquiry or investigation determines that a compromise occurred, the official initiating the inquiry or investigation shall immediately notify the originator (i.e., the OCA) of the

1804 information or material involved. The OCA(s) shall take the actions required by section 9 of this
1805 enclosure.

1806
1807 (2) If the originating activity no longer exists, the activity that inherited the functions of
1808 the originating activity shall be notified. If the functions of the originating activity were dispersed
1809 to more than one other activity, the inheriting activity(ies) cannot be determined, or the functions
1810 have ceased to exist, the senior agency official of the DoD Component of which the originating
1811 activity was a part shall be notified. This notification shall not be delayed pending completion of
1812 any additional inquiry or investigation or resolution of other related issues.

1813
1814 d. Security Inquiries. The head of the activity or activity security manager having security
1815 cognizance shall initiate an inquiry into the actual or potential compromise promptly to determine
1816 the facts and circumstances of the incident, and to characterize the incident as an infraction or a
1817 violation. At conclusion of the inquiry, a narrative of findings is provided in support of
1818 recommended additional investigative or other actions by the activity.

1819
1820 (1) The official appointed to lead the inquiry shall not be anyone involved with the
1821 incident. Preferably, the security manager should not be appointed to lead the inquiry.

1822
1823 (a) ***(Added)(DAF) The commander or director must appoint an inquiry official,**
1824 **in writing, within three (3) duty days from the discovery of the security incident; or, the**
1825 **following duty day if the incident occurs on a Friday, weekend or holiday. (T-1). Every**
1826 **attempt should be made to ensure these individuals are equal to, or higher in rank/grade,**
1827 **than the suspected culpable parties involved in the incident. Inquiry officials will not be a**
1828 **person assigned to the IP office (MAJCOM/FLDCOM or installation), or activity security**
1829 **manager. (T-1). The individual must be cleared to the highest level of information involved;**
1830 **or, be given one-time access in accordance with Reference (cl). (T-0).**

1831
1832 (b) ***(Added)(DAF) Depending on the circumstances, formal appointment of an**
1833 **inquiry official may not be warranted. The commander, director or activity security**
1834 **manager (security assistant) will consult with the servicing IP office to determine if an**
1835 **informal inquiry can be conducted. (T-1). If determined appropriate, a memorandum for**
1836 **record (MFR) would alleviate the need to conduct a formal inquiry, which requires an**
1837 **appointment letter, generating an inquiry report, conducting a technical review, and issuing a**
1838 **closure memorandum. For example, a security infraction that does not result in a loss or**
1839 **compromise of classified information, can be closed by completion of a MFR, signed by the**
1840 **activity security manager (security assistant). In such cases, the MFR will include sufficient**
1841 **detail to support the “no loss or compromise” determination.**

1842
1843 (c) **(Added)(DAF) The commanders or director shall not approve, endorse, and**
1844 **close inquiry reports until after a technical review, by the servicing IP Office, has been**
1845 **completed. (T-1). The final report will include the following, at minimum. (T-1).**

1846
1847 **1. (Added)(DAF) Concurrence in whole or part with the findings.**

1848
1849 **2. (Added)(DAF) Classification of the information and the applicable SCG.**

1850
1851 **3. (Added)(DAF) If an actual, potential or suspected loss or compromise**
1852 **occurred or did not occur and whether or not further investigation is needed.**

1853
1854 **4. (Added)(DAF) Classification of the incident as a security violation or**
1855 **infraction.**

1856
1857 **5. (Added)(DAF) Corrective actions to prevent further occurrences are**
1858 **appropriate and if necessary, incorporate the actions into the security plan.**

1859
1860 **6. (Added)(DAF) Any administrative, disciplinary or punitive action taken**
1861 **against individual(s) responsible for the violation if warranted. This may include verbal**
1862 **counseling and/or remedial training, if this is deemed more appropriate for the situation.**

1863
1864 **7. (Added)(DAF) If the OCA was notified to complete a damage assessment.**

1865
1866 **8. (Added)(DAF) Statement citing whether the incident was caused by**
1867 **willful, negligent or inadvertent action.**

1868
1869 (2) An inquiry shall be initiated and completed as soon as possible, not to exceed 10 duty
1870 days, and a report of findings provided to the activity head, activity security manager, and others as
1871 appropriate. If the inquiry cannot be completed within 10 duty days an extension should be
1872 requested from the appointing official.

1873
1874 (3) No recommendation should be made by an inquiry officer with regard to punitive
1875 action against the individual(s) responsible for the violation. An inquiry officer's function is to
1876 determine and report facts and make recommendations for actions needed to prevent future
1877 violations of the type investigated. Disciplinary or punitive action is the responsibility of the
1878 appropriate military commander or management official.

1879
1880 **(a) *(Added)(DAF) The servicing IP office will provide guidance and assistance**
1881 **to commanders, directors, and inquiry officials, as necessary. (T-1). The commander or**
1882 **director must ensure that information indicating willful or negligent behavior, for any**
1883 **culpable parties, is recorded in DISS (or its successor system) and transmit the closed inquiry**
1884 **or investigation report to the DoD Consolidated Adjudication Facility. (T-1). Determining if**
1885 **the incident warrants reporting to the counter-insider threat hub is also required.**

1886
1887 **(b) (Added)(DAF) The servicing IP office shall be notified if an extension is**
1888 **granted, for tracking purposes. (T-1).**

1889
1890 (4) If information obtained as a result of the inquiry is sufficient to provide answers to the
1891 following questions, then such information shall be sufficient to resolve the incident, to include
1892 instituting administrative sanctions consistent with section 17, Enclosure 3 of Volume 1 of this
1893 Manual.

1894
1895 (a) When, where, and how did the incident occur? What persons, situations, or
1896 conditions caused or contributed to the incident?

1897
1898 (b) Was classified information compromised?

1899
1900 (c) If a compromise occurred, what specific classified information and/or material was
1901 involved? What is the classification level of the information disclosed?

1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950

(d) If classified material is alleged to have been lost, what steps were taken to locate the material?

(e) Was the information properly classified?

(f) Was the information officially released?

(g) In cases of compromise involving the public media:

1. In what specific media article, program, book, Internet posting or other item did the classified information appear?

2. To what extent was the compromised information disseminated or circulated?

3. Would further inquiry increase the damage caused by the compromise?

(h) Are there any leads to be investigated that might lead to identifying the person(s) responsible for the compromise?

(i) If there was no compromise, and if the incident was unintentional or inadvertent, was there a specific failure to comply with established security practices and procedures that could lead to compromise if left uncorrected and/or is there a weakness or vulnerability in established security practices and procedures that could result in a compromise if left uncorrected? What corrective action is required?

e. Security Investigations. If the circumstances of an incident require a more detailed or additional investigation, then an individual shall be appointed by the activity head in writing, to conduct that investigation and, as appropriate, provide recommendations for any corrective or disciplinary actions.

f. *(Added)(DAF) If the security incident warrants a security investigation, the servicing IP office will coordinate with the local OSI field office to ascertain if a CI or criminal investigation is warranted, in conjunction with or in lieu of. (T-1). If a CI or criminal investigation is initiated, it will take precedence over the security investigation. If a CI or criminal investigation is not initiated, the investigating officer should maintain close coordination with and consult the local OSI detachment, Office of the Staff Judge Advocate, or security forces squadron for guidance throughout the process.

(1) The individual appointed shall be sufficiently senior to ensure a successful completion of the investigation and should be commensurate with the seriousness of the incident; have an appropriate security clearance; have the ability to conduct an effective investigation; and shall be someone unlikely to have been involved, directly or indirectly, in the incident.

(2) Except in unusual circumstances, the activity security manager shall not be appointed to conduct the investigation.

(3) As an investigation may lead to administrative or disciplinary action, the evidence developed should be comprehensive in nature and gathered in such a manner that it would be

1951 admissible in a legal or administrative proceeding. Consult local legal counsel as needed for
1952 procedural guidance on conduct of the investigation.

1953
1954 (4) The investigation should be accomplished promptly following appointment of the
1955 investigating officer. The results of the investigation shall be documented in writing. The format
1956 in Appendix 1 to this enclosure may be used.

1957
1958
1959 7. INFORMATION APPEARING IN THE PUBLIC MEDIA

1960
1961 a. If classified information appears in the public media, including on public Internet sites, or if
1962 approached by a representative of the media, DoD personnel shall be careful not to make any
1963 statement or comment that confirms the accuracy of or verifies the information requiring
1964 protection. Report the matter as instructed by the appropriate DoD Component guidance, but do
1965 not discuss it with anyone who does not, in the case of classified information, have an appropriate
1966 security clearance and need to know.

1967
1968 b. If the fact of an unauthorized public disclosure becomes widely known, the Component
1969 senior agency official should consider whether the workforce needs to be reminded of actions to be
1970 or not to be taken by individuals in response to the disclosure. Reminders may include such topics
1971 as not viewing or downloading the classified information from unclassified IT systems, not
1972 confirming the accuracy of the information, and providing a point of contact for media inquiries.

1973
1974 c. Notifications of unauthorized disclosures of classified information in the public media
1975 required by subparagraph 3.f.(1)(b) of this enclosure shall include the information specified in
1976 subparagraphs 7.c.(1) through 7.c.(7). Initial notifications providing basic information about the
1977 incident and a point of contact should be made as quickly as is feasible; complete information
1978 should be provided subsequently.

1979
1980 (1) Date, location, and author of the public media item.

1981
1982 (2) Specific information disclosed and its classification level.

1983
1984 (3) Identification of the OCA.

1985
1986 (4) The extent to which the disclosed information was circulated, both within and outside
1987 the DoD, and the number of persons known to have had access to the information.

1988
1989 (5) An appraisal of or statement regarding the damage to national defense and/or national
1990 security programs caused by the disclosure.

1991
1992 (6) A statement of whether any investigative leads exist and what additional actions, if
1993 any, are contemplated (i.e., no further action; administrative investigation by the DoD Component;
1994 referral to the cognizant DCIO for criminal investigation; or a request for USD(I&S) referral to DoJ
1995 for investigation).

1996
1997 (7) Point of contact for further information.

1998
1999 d. When notified of a suspected compromise of classified information through the public

media, the USD(I&S) shall, unless already done by the reporting DoD Component, consult with the Assistant Secretary of Defense for Public Affairs and other officials having a primary interest in the information to determine if the information was officially released under proper authority.

e. When responsibility for an inquiry into an unauthorized public media disclosure is unclear or is shared equally with another DoD Component, refer the matter through security channels to the USD(I&S) who shall decide investigative responsibility in consultation with the affected DoD Components.

f. The decision on whether to initiate an additional investigation by a DCIO or by the Federal Bureau of Investigation through a referral to the DoJ shall be based on the following factors:

(1) The accuracy of the information disclosed.

(2) The damage to national security caused by the disclosure and whether there were compromises regarding sensitive aspects of current classified projects, intelligence sources, or intelligence methods.

(3) The extent to which the disclosed information was circulated, both within and outside the DoD, and the number of persons known to have access to it.

(4) The degree to which an investigation shall increase the damage caused by the disclosure.

(5) The existence of any investigative leads.

(6) The reasonable expectation of repeated disclosures.

g. If the DoD Component's initial inquiry or investigation or a DCIO investigation identifies the person(s) responsible for an unauthorized disclosure of classified information via the public media or Internet, the DoD Component shall notify the Director of Security, USD(I&S). This notification shall include responses to the DoJ Media Leak Questionnaire (see Appendix 2 of this enclosure). USD(I&S), in coordination with the General Counsel of the Department of Defense (GC, DoD) and the Head of the DoD Component having OCA, shall decide whether additional investigation is appropriate and whether to refer the unauthorized disclosure to the DoJ for investigation and/or criminal prosecution. When the initial inquiry or investigation does not identify the person responsible, the Head of the DoD Component, in consultation with the USD(I&S) and the GC, DoD, shall decide if further investigation is appropriate.

8. RESULTS OF INQUIRIES AND INVESTIGATIONS

a. If the conclusion of the inquiry or investigation is that a compromise occurred and that weakness or vulnerability in established security practices and/or procedures contributed to the compromise or that the potential exists for a compromise of classified information due to a weakness or vulnerability in established security practices and/or procedures, the appropriate responsible security official shall take prompt action to issue new or revised guidance, as necessary, to resolve identified deficiencies. Results of inquiries and/or investigations into actual or potential compromises that indicate that defects in the procedures and requirements of this Manual

2049 contributed to the incident shall be reported to the Director of Security, USD(I&S).

2050
2051 b. If the conclusion of the inquiry or investigation is that a compromise did not occur, but that
2052 there was potential for compromise of classified information due to a failure of a person or persons
2053 to comply with established security practices and/or procedures, the official having security
2054 responsibility over such persons shall be responsible for taking action as may be appropriate to
2055 resolve the incident.

2056
2057 c. Additional investigation, beyond what is required by this enclosure, may be needed to
2058 permit application of appropriate sanctions for violation of regulations, criminal prosecution, or
2059 determination of effective remedies for discovered vulnerabilities. The inquiry this enclosure
2060 requires may serve as part of these investigations, but notifying OCAs shall not be delayed pending
2061 completion of these additional investigations.

2062
2063
2064 9. ACTIONS TO BE TAKEN BY THE OCA. When notified of the compromise of classified
2065 information, the OCA shall:

2066 a. Verify the classification and duration of classification initially assigned to the information.

2067
2068 b. Reevaluate the classification assigned to determine whether the classification shall be
2069 continued or changed. This classification review shall consider the following possibilities:

2070
2071 (1) The information has lost all or some of its sensitivity since it was initially classified
2072 and should be downgraded or declassified (in rare cases, it might also be discovered that the
2073 information has gained sensitivity and should be upgraded).

2074
2075 (2) The information has been so compromised by the incident that attempting to protect it
2076 further as classified is unrealistic or inadvisable, and it should be declassified.

2077
2078 (3) The information should continue to be classified at its current level.

2079
2080 c. Advise the activity reporting the compromise of the outcome of the classification
2081 assessment required by paragraphs 9.a and 9.b of this section within 72 hours of notification.

2082
2083 d. Assess the impact of the compromise on the affected system, plan, program, or project;
2084 consider countermeasures (e.g., damage control actions) that may be taken to minimize, mitigate or
2085 limit damage to national security and prevent further loss or compromise; and then initiate or
2086 recommend adoption of such countermeasures.

2087
2088 (1) Where appropriate, countermeasures should be applied as quickly as possible and may
2089 be initiated prior to completion of the classification review or damage assessment.

2090
2091 (2) Countermeasures could include changing plans or system design features, revising
2092 operating procedures, providing increased protection to related information (e.g., classification
2093 upgrading), or other appropriate actions.

2094
2095 (3) Evaluate the cost implications of information, operational, or technology losses;
2096 developmental and integration costs of countermeasures; likelihood of countermeasure success; and
2097

2098 programmatic impacts of the unmitigated loss and/or compromise of specific classified
2099 information.

2100
2101 e. Conduct a damage assessment as required by section 10 of this enclosure to determine the
2102 effect of the compromise of classified information on the national security.

2103
2104
2105 10. DAMAGE ASSESSMENTS

2106
2107 a. A damage assessment is undertaken to determine the effect of a compromise on the national
2108 security.

2109
2110 (1) A damage assessment shall normally consist of a detailed, multidisciplinary
2111 examination of the facts surrounding the compromise to determine the practical effects of a
2112 compromise on DoD programs, operations, systems, materials, and intelligence and on the DoD's
2113 ability to conduct its missions; to address mitigations and countermeasures that could be put in
2114 place to decrease or offset the impact; to determine the estimated dollar costs to implement
2115 countermeasures essential to maintain or reinstate security, or to replace weapons systems or
2116 capabilities that are thoroughly compromised; and to provide, when appropriate, specific
2117 recommendations for action.

2118
2119 (2) A damage assessment is conducted after the classification review and often follows
2120 any prosecutorial actions. However, when necessary to identify damage done by the disclosure or
2121 otherwise appropriate, a damage assessment may be conducted pre-prosecution.

2122
2123 (3) The damage assessment is not to be confused either with the classification review
2124 performed by the OCA or with damage control actions, which are those actions performed
2125 immediately upon the discovery of disclosure or compromise to minimize risk, limit damage,
2126 and/or prevent further loss or compromise.

2127
2128 b. Each DoD Component shall establish a system of controls and internal procedures to ensure
2129 that damage assessments are conducted, at a minimum, for cases of compromise involving
2130 espionage, intelligence information or compromise via the public media. Damage assessments are
2131 encouraged for other compromises.

2132
2133 (1) Conduct of the damage assessment is the responsibility of the OCA and subject matter
2134 experts. Security officials should provide assistance as needed and appropriate.

2135
2136 (2) The results of relevant security inquiries and investigations shall be made available to
2137 inform the damage assessment process, as needed. Reports of criminal or CI investigations
2138 associated with the compromise should be requested by the OCA from the cognizant DCIO or
2139 Defense CI component.

2140
2141
2142 11. VERIFICATION, REEVALUATION, AND DAMAGE ASSESSMENT TIMELINES. The
2143 verification and reevaluation steps in section 9 of this enclosure, and when appropriate the damage
2144 assessment process in section 10 of this enclosure, shall be completed as soon as possible following
2145 notification of a compromise. However, damage assessments requiring multi- disciplinary or
2146 multiple agency review of the adverse effects of the compromise on systems, operations, and/or

2147 intelligence, may sometimes be a long-term process. The DoD goal for completion of a damage
2148 assessment involving compromised classified information is no longer than 6 months from the first
2149 date the compromise was declared. Accomplishment of the assessment prior to the initiation of
2150 legal or administrative proceedings may be beneficial; check with legal counsel.

2151
2152
2153 **12. ACTUAL OR POTENTIAL COMPROMISES INVOLVING MORE THAN ONE AGENCY.**

2154 When classified information under the control of more than one DoD Component or another
2155 Federal agency is involved, the affected activities are responsible for coordinating their efforts in
2156 evaluating the classification of information involved and assessing damage.

2157
2158
2159 **13. DEBRIEFING IN CASES OF UNAUTHORIZED ACCESS.** In cases where unauthorized
2160 access to classified information has occurred, it may be advisable to discuss the situation with the
2161 individual(s) to enhance the probability that he or she shall properly protect it. The activity head
2162 shall determine if a debriefing is warranted. This decision shall be based on the circumstances of
2163 the incident, what is known about the person(s) involved, and the nature of the information. The
2164 following general guidelines apply:

2165
2166 a. If the unauthorized access was by a person with the appropriate security clearance but no
2167 need to know, debriefing is usually appropriate only so far as necessary to ensure that the
2168 individual is aware that the information to which they had unauthorized access is classified and
2169 requires protection.

2170
2171 b. If the unauthorized access was by U.S. Government civilian or military personnel or an
2172 employee of a U.S. Government contractor, who does not have a security clearance, debriefing is
2173 usually appropriate. The person shall be advised of his or her responsibility to prevent further
2174 dissemination of the information and of the administrative sanctions and criminal penalties that
2175 might follow if he or she fails to do so. The debriefing shall be designed to ensure that the
2176 individual understands the nature of the information, why its protection is important, and knows
2177 what to do if someone tries to obtain the information. In the case of non-DoD U.S. Government
2178 personnel and employees of U.S. Government contractors, the appropriate security official in the
2179 individual's parent organization, including the appropriate facility security officer where
2180 applicable, shall be advised of the debriefing.

2181
2182 c. If the person involved is neither a member of a U.S. Government organization nor an
2183 employee of a U.S. Government contractor, the decision is much more situational. The key
2184 question is whether the debriefing shall have a positive effect on the person's ability or willingness
2185 to protect the information.

2186
2187 d. In any case where the person to be debriefed may be the subject of criminal prosecution or
2188 disciplinary action, consult with legal counsel before attempting to debrief the individual.

2189
2190 e. It is sometimes useful to have the person being debriefed sign a statement acknowledging
2191 the debriefing and his or her understanding of its contents, or to execute a SF 312. If an NDA is
2192 not executed, the nature and format of the statement is left to the discretion of the local security
2193 official to allow flexibility in meeting the requirements of a particular incident. If the person
2194 refuses to sign an NDA or debriefing statement when asked, this fact and his or her stated reasons
2195 for refusing shall be made a matter of record in the inquiry.

2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223

14. REPORTING AND OVERSIGHT MECHANISMS. The DoD Components shall establish necessary reporting and oversight mechanisms to ensure that inquiries and/or investigations are conducted when required, that they are done in a timely and efficient manner, and that appropriate management action is taken to correct identified problems. Inquiries or investigations and management analyses of security incidents shall consider possible systemic shortcomings that may have caused or contributed to the incident. The effectiveness of activity security procedures, security education, supervisory oversight of security practices, etc., shall be considered in determining causes and contributing factors. The focus of management response to security incidents shall be to eliminate or minimize the probability of further incidents occurring. Appropriate disciplinary action or legal prosecution, as discussed in section 17, Enclosure 3 of Volume 1 of this Manual, is sometimes one means of doing this, but the broader focus on prevention shall not be lost. Simple disciplinary action, without consideration of what other factors may have contributed to the situation, shall not be considered an acceptable response to a security incident.

15. ***(Added)(DAF) Each IP office will keep a rolling total of all security incidents (broken-out by infractions and violations) for their activity, throughout the fiscal year, and submit this information to the MAJCOM/FLDCOM Director, IP, upon request. (T-1). Use the Security Incident Tracker at appendix 3, to this enclosure, to capture all required data elements; do not report the same incident more than once. (T-1).**

Appendixes

1. Security Incident Reporting Format
2. DOJ Media Leak Questionnaire
3. ***(Added)(DAF) Security Incident Tracker**

2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238

APPENDIX 1 TO ENCLOSURE 6

SECURITY INCIDENT REPORTING FORMAT

1. The report format, as described in Figure 2 is optional, to be used as a guide for appropriate content. The format may be used as shown or tailored to suit the organization and the circumstances. In all cases, the goal is to identify who, what, when, where, why, and how the incident occurred and to determine what should be done to preclude similar incidents in the future.
2. Classify, and appropriately mark, security incident reports according to content. At a minimum, reports shall be designated and marked “CUI,” as the reports will contain information on personnel involved. The reports may also contain other information that qualifies for designation as CUI and information that could facilitate unauthorized access to classified information.

2239
2240

2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289

2290
2291

FIGURE 2. REPORT OF SECURITY INCIDENT INQUIRY OR INVESTIGATION

TO: Official Initiating Inquiry or Investigation (e.g., Activity Security Manager or Activity Head) (others as required)

THRU: (Appropriate chain of command)

SUBJECT: Report of Security Incident Inquiry or Investigation

1. Summary. A summary of who, what, when, where, why, and how the violation occurred. (Also see DoD Manual 5200.01-V3, section 6 of Enclosure 6.)

2. Sequence of Events. A detailed sequence of events tracing the security violation from start to finish. This sequence will include a list of all personnel (include name, grade, social security number (for positive identification and adverse information reporting), position, organization, clearance eligibility level, and access authorized) involved in order of their specific time of involvement; and all locations involved.

a. Indicate date of violation’s discovery and likely occurrence (if known). Identify the material (e.g., documents, information, or equipment) involved in the violation. Identify individuals not cleared for classified information and the extent of exposure. Identify procedural problems or other factors that may have contributed to the violation.

b. Provide a detailed description of the information involved in the incident. Include classification, compartment levels, caveats and any control or dissemination notices; identification of the material (e.g., message, letter, staff study, imagery, magnetic media, equipment item) by subject and date or nomenclature, to include any control/serial numbers; originating office and OCA; and volume of material (e.g., number of pages or items of equipment) involved.

c. Make a statement as to the likelihood of compromise. If material has been compromised, identify the extent of compromise and state the date or time period during which information was lost or compromised. Identify by name the individual(s) and organization(s) of personnel at fault for, or contributing to, the violation, if possible, and reason(s) they are culpable or contributed to the occurrence of a violation.

d. Identify deficient procedure(s) and describe how they led or contributed to the incident (too vague, weak, out-of-date, unenforceable, ineffective, etc.). Include any assessment regarding systemic weaknesses or vulnerabilities in established security practices (e.g., non-existent, out-of-date, or ineffective policies, procedures or training) that must be corrected; suggest the corrective actions required.

3. Actions taken. List actions that have been taken (e.g., notifications made, messages sent, interviews with, counseling of, and discipline rendered for individuals involved, and other information as required). Include dates inquiry or investigation started and ended.

4. Recommendations. Make recommendations concerning what should be done to preclude future incidents of this type.

5. Identification of inquiry or investigating official, organization, and telephone numbers.

6. Evaluation notes. Enter other information relevant to the inquiry or investigation. Attach interview statements and/or records, documentary evidence, exhibits and so forth, as appropriate.

(Signature of Inquiry or Investigating Official)

CUI (or, if classified, insert classification and add other markings as required)

APPENDIX 2 TO ENCLOSURE 6

DOJ MEDIA LEAK QUESTIONNAIRE

1. If the initial inquiry and/or investigation into an unauthorized disclosure of classified information via the media identifies the person responsible for the unauthorized disclosure, the Head of the DoD Component shall promptly answer to the fullest extent possible the standard questions in this appendix, which comprise the DoJ Media Leak Questionnaire, and submit the questionnaire through security channels to the USD(I&S). In coordination with the GC, DoD, the USD(I&S) shall, when warranted, forward the information via letter to:

Department of Justice, Criminal Division
Attention: Chief, Internal Security Section Bond Building, Room 9400
1400 New York Avenue, NW
Washington, DC 20530

a. What is the date and identity of the media source (e.g., article, blog, television, or other oral presentation) containing classified information?

b. What specific statement(s) in the media source are classified and was the information properly classified?

c. Is the classified information disclosed accurate?

d. Did the information come from a specific document, and if so, what is the origin of the document and the name of the individual responsible for the security of the classified data discussed?

e. What is the extent of official circulation of the information?

f. Has the information been the subject of prior official release?

g. Was prior clearance for publication or release of the information sought from proper authorities?

h. Has the material, parts thereof or enough background data, been published officially or in the press to make an educated speculation on the matter possible?

i. Will the information be made available for use in a prosecution, and if so, what is the name of the person competent to testify on its classification?

j. Was declassification considered or decided on before the data appeared in the media?

k. What effect might the disclosure of the classified data have on the national defense?

2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384

***(Added)(DAF) APPENDIX 3 TO ENCLOSURE 6**

***(Added)(DAF) SECURITY INCIDENT TRACKER**

1. *(Added)(DAF) BACKGROUND

a. *(Added)(DAF) In an effort to better implement and enforce procedures to prevent the unauthorized disclosure of classified information, a new security incident tracker has been developed to aid in the uniform collection of data. Security incidents must be closely monitored and tracked to determine root causes and develop mitigating strategies that help prevent future occurrences. (T-1).

b. *(Added)(DAF) A data spill of classified information is considered a security violation, per DEPSECDEF Memorandum, *Unauthorized Disclosures of Classified Information or Controlled Unclassified Information on DoD Information Systems*. Therefore, every data spill is an unauthorized disclosure (UD) and an incident category shall be assigned in the tracker. (T-0). Identification or categorization of a UD is not determined by how quickly the data spill is (can be) mitigated.

c. *(Added)(DAF) For all security incidents categorized as willful or negligent, a final copy of the inquiry report shall be forwarded to the servicing personnel security office to execute reporting requirements in DISS (or successor system) under the continuous evaluation program, per reference (cl) and *Security Executive Agent Directive 4*, (reference (cv)). (T-0).

2. *(Added)(DAF) INSTRUCTIONS

a. *(Added)(DAF) Populate each field, based on the below criteria, for all security incidents that occurred within each fiscal year (FY). The matrix can be converted to MS Excel, for ease of use.

- *(Added)(DAF) Column 1. Reporting Activity**
- *(Added)(DAF) Column 2. Date of Incident**
- *(Added)(DAF) Column 3. Date Incident Report Closed**
- *(Added)(DAF) Column 4. Date MAJCOM/FLDCOM/Wing Notified**
- *(Added)(DAF) Column 5. Incident Type**
- *(Added)(DAF) Column 6. Incident Category**
- *(Added)(DAF) Column 7. Actual or Potential Loss or Compromise**
- *(Added)(DAF) Column 8. Classification Level**
- *(Added)(DAF) Column 9. Incident Description (*must be unclassified*)**
- *(Added)(DAF) Column 10. Association Type**
- *(Added)(DAF) Column 11. Incident reported in DISS for all culpable party(ies). If no, explain why in the notes column**
- *(Added)(DAF) Column 12. Corrective Actions Taken (e.g., remedial training; updated procedures; loss of access)**
- *(Added)(DAF) Column 13. Notes**
- Bottom Row. Totals for Columns 5 – 8, 10, 11**

****CLASSIFICATIONS AND EXAMPLES LISTED IN THE TABLE ARE FOR INSTRUCTIONAL PURPOSES ONLY****

Keep a rolling total of all security infractions and violations and submit the data, as requested. (T-1). Use these categories (Column 9) for reporting purposes and identify the area most impacted. *Do not report the same infraction/violation*

1	2	3	4	5	6	7	8	9	10	11	12	13
Reporting Activity	Date of Incident	Date Incident Report Closed	Date MAJCOM/FL DCOM / WING Notified	Incident Type	Incident Category	Actual or Potential Loss or Compromise	Classification Level	Incident Description	Association Type	Reported in DISS?	Corrective Actions Taken	Notes
	YYYYMMDD	YYYYMMDD	YYYYMMDD	Infraction or Violation	Inadvertent, Negligent or Willful	Yes or No	Top Secret Secret Confidential	1. Unauthorized Access 2. Data Spill 3. Improper Classification 4. Improper Storage 5. Improper Transmission/Transportation 6. Improper Destruction 7. Unauthorized Reproduction 8 Prohibited Device 9. Other- Explain	Military, Civilian or Contractor	Yes or No N/A		
XYZ-111 Fighter Squadron	20210120	20210130	N/A	VIOLATION	NEGLIGENT	NO	CONFIDENTIAL	5. IMPROPER TRANSMISSION/TRANSPORTATION	Contractor	NO SEE NOTES	ALL-HANDS REMINDER SENT OUT ON PROCESS; LOCAL COURIER CARD SOP UPDATED; REMEDIAL TRAINING PROVIDED	COR AND FSO WERE NOTIFIED TO TAKE ACTIONS IN DISS
ABC-789 Fighter Squadron	20210205	20210206	N/A	INFRACTION	N/A	NO	SECRET	8. OTHER – INDIVIDUAL DID NOT USE A COVERSHEET WHEN COLLECTING CLASSIFIED DOCUMENTS FROM THE PRINTER	Military	N/A	REMEDIAL TRAINING PROVIDED	
XYZ-333 Fighter Squadron	20210207	20210215	N/A	INFRACTION	N/A	NO	SECRET	8. OTHER – SECURE ROOM IDS WAS ACTIVATED, BUT THE HIGH-SECURITY LOCK ON THE DOOR WAS NOT ENGAGED SEE NOTES	Military	N/A	REMEDIAL TRAINING PROVIDED	IDS LOGS SHOW NO ONE ACCESSED THE SPACE UNTIL THE FOLLOWING MORNING; BUILDING HAS A 24/7 GUARD FORCE
XYZ-222 Fighter Squadron	20210410	20210430 SEE NOTES	20210430	VIOLATION	NEGLIGENT	YES	TOP SECRET	2. DATA SPILL	Civilian	YES	RESUME WAS REMOVED FROM THE SITE & INDIVIDUAL'S PROFILE WAS DEACTIVATED; REMEDIAL TRAINING PROVIDED; LOSS OF NETWORK ACCESS FOR 5 DAYS	EXTENSION WAS GRANTED ON 20210421
TOTALS				I = 2 V = 2	I = 0 N = 1 W = 0	I	C = 1 S = 2 TS = 1		MIL = 2 CIV = 1 CONT = 1	Y = 1 N = 1 N/A = 2		

in more than one area.

- 1. Unauthorized Access.** Occurs when, unauthorized personnel accessed or had opportunity to access classified material. This includes, but is not limited to: individuals with a clearance eligibility, but do not have a valid need-to-know or authorized access; and, sharing classified passwords, tokens, PINs, or other access credentials permitting access into classified areas or classified systems.
- 2. Data Spill.** Occurs when, classified data is introduced either onto an unclassified information system or to an information system with a lower level of classification, or to a system not accredited to process data of that restrictive category.
- 3. Improper Classification.** Improper original and derivative classification decisions, classification level designations, and/or classification actions, including incorrect/missing markings that caused mishandling of classified information.
- 4. Improper Storage.** Unsecured documents, equipment or secure rooms; or, unauthorized storage containers.
- 5. Improper Transmission/Transportation.** Transmitting or transporting classified via unsecured or unapproved means (other than through IT systems), improper hand-carrying, not properly packaged, and classified discussions over unsecured lines.
- 6. Improper Destruction.** Destruction by unauthorized means (i.e., the destruction equipment is not on the NSA/CSS evaluated products list (EPL)).
- 7. Unauthorized Reproduction.** Reproduction by unauthorized means; or, reproducing material not authorized for reproduction.
- 8. Prohibited Device.** The introduction of a cell phone, PED, 2-way pager, and other electronic devices into a secure/restricted area; during a classified discussion or meeting; during a classified test vent; etc.
- 9. Other.** Incident that does not fit into one of the above categories.

IT ISSUES FOR THE SECURITY MANAGER

1
2
3
4
5
6 1. OVERVIEW. This enclosure identifies and discusses the most common IT issues facing
7 security organizations and provides references and pointers to the relevant primary sources. As the
8 Internet, classified and unclassified networks, and a wide range of computer systems are used in
9 every facet of the operation of the DoD, challenges and questions related to IT issues and the
10 interaction between the security and IT staffs abound. The traditional security manager's portfolio,
11 planning horizon, and focus on classification management and personal, physical, and operational
12 security issues no longer suffice. The continuing protection and security of complex IT and
13 information systems depends upon a robust and effective interaction and coordination between
14 security and IT organizations.

15
16
17 2. RESPONSIBILITY. In accordance with Reference (b), overall security responsibility for
18 protection of classified information and CUI remains with the information security program and
19 staff, even though the data and/or information resides on IT and information systems and networks
20 managed and controlled by the DoD Component CIO. Accordingly, proactive and continuous
21 engagement and collaboration between security, IT, and IA professionals, at all organizational
22 levels, is essential in order to ensure the protection of DoD information as well as the Department's
23 electronic enterprise.

24
25
26 3. IA ROLES AND FUNCTIONS

27
28 a. In accordance with Reference (v) and DoDD 8000.01 (Reference (bq)), IA and IT policy
29 and information systems operations are the purview of the CIO of the DoD at the OSD level and
30 the counterpart organizations in the DoD Components.

31
32 b. U.S. Strategic Command, through U.S. Cyber Command (USCYBERCOM), has the overall
33 responsibility for directing the operation of and assuring the security of the global DoD network
34 environment. USCYBERCOM will lead the day-to-day defense and protection of the DoD
35 networks and will coordinate all DoD network operations, providing full spectrum support to
36 military and counterterrorism missions.

37
38 c. At the DoD Component and activity level, there are several important IA roles and
39 functions that security managers need to recognize and understand to develop a productive
40 relationship with the IA staff, including the authorizing official (AO), IT AO, and IA officer (IAO).
41 The glossary provides definitions of these functions and identifies other titles that are sometimes
42 used for these same functions.

43
44
45 4. IA CONCEPTS

46
47 a. IA Attributes. All DoD information systems are to maintain appropriate levels of
48 availability, integrity, authentication, confidentiality, and non-repudiation in order to protect and
49 defend DoD information and networks. While all five of these attributes are critical to the user's

50 ability to perform the assigned mission, from an information security perspective, confidentiality
51 and authentication may be the most important.

52
53 (1) The loss of availability means that the information system, computer network, and/or
54 data are unavailable to authorized users, and missions or operations cannot be performed. Loss of
55 availability within a computing environment may be an extremely serious event, depending on the
56 criticality of the applications and missions supported.

57
58 (2) The loss of integrity means that the data can no longer be trusted to be reliable or
59 accurate.

60
61 (3) Authentication is critical, as it is the mechanism that authorizes or allows access to
62 computer systems and networks and the data that resides there. Loss of or incorrect authentication
63 services could allow unauthorized access to classified data.

64
65 (4) The loss of confidentiality means that data may be available in an electronic form to
66 users who are not authorized to receive it. Depending on the classification level of the system or
67 network, loss of confidentiality could mean a compromise of classified information.

68
69 (5) The loss of non-repudiation assurances means that authorized users no longer can be
70 certain with whom they are communicating because general communications (and therefore the
71 data processed by that information system) cannot be trusted or verified.

72
73 b. System Categorization. Each information system must be categorized and have appropriate
74 IA controls assigned in accordance with Reference (v). System categorization requires
75 determination of the potential impacts of the loss of confidentiality, integrity, and availability
76 associated with the specific system or information. IA controls are selected based on the results of
77 the system categorization process. Security personnel may find it helpful to understand the
78 categorization of the DoD information system(s) within their area of responsibility, as those
79 designations impact the information, physical, personal, and operational security environment and
80 the resource requirements that must be dedicated to protection of the system(s) and the information
81 processed.

82
83 c. Assessment and Authorization (A&A). A&A of DoD systems is governed by Reference (s).

84
85 (1) Certification is the comprehensive evaluation of the technical and nontechnical (e.g.,
86 procedural) security safeguards of an information system undertaken to support the accreditation
87 process. It establishes the extent to which a particular design and implementation meets a set of
88 specified security requirements.

89
90 (2) Accreditation is the formal declaration by a AO that, based on the implementation of a
91 specified set of technical, managerial, and procedural safeguards, the level of risk is acceptable and
92 the information system is approved to operate at a specific security level.

93
94 (3) The security manager and the AO should coordinate with each other during the A&A
95 process. The AO needs to work with the security organization to ensure an understanding of the
96 security requirements that must be met based on the classification of the information to be
97 processed, and for identification of any security issues associated with the operation of the system.
98 The security staff, on the other hand, must be aware of the nature, scope, and schedule of ongoing

99 A&A activities within a given organization, in order to provide timely and relevant classification
100 management direction and to ensure the physical environment is properly secured and accredited
101 for the operations planned and that users are properly cleared and have all requisite access in time
102 to support the mission.

105 5. DATA SPILLS

107 a. Classified data spills occur when classified data is introduced either onto an unclassified
108 information system or to an information system with a lower level of classification, or to a system
109 not accredited to process data of that restrictive category. Although it is possible that no
110 unauthorized disclosure occurred, classified data spills are considered and handled as a possible
111 compromise of classified information involving information systems, networks, and computer
112 equipment until the inquiry determines whether an unauthorized disclosure did or did not occur.

114 b. When a classified data spill occurs, the activity security manager is responsible ensuring
115 that the policy requirements for addressing an unauthorized disclosure, as specified in Enclosure 6
116 or other provisions of this Manual, are met (e.g., inquiry, notification, investigation, damage
117 assessment); however, these responsibilities must be carried out in close coordination with the IT
118 and/or IA staff, which has overall responsibility for the operation of the networks and systems as
119 well as the technical knowledge needed to address the spill. Security personnel have the overall
120 lead for addressing such events.

122 c. CNSS Policy 18 (Reference (br)) applies to the spillage of classified national security
123 information on any information system, be it government, contractor, or privately owned, and
124 provides a policy framework for the consistent handling of the spillage. Each Federal Government
125 organization that owns or operates classified information systems is required to establish policies
126 and procedures for handling classified information spillage. When a classified data spill occurs,
127 Reference (br) requires that it is immediately:

129 (1) Reported to the appropriate authorities, including, at a minimum, the OCA, the
130 information owner/originator, the IAM, the activity security manager, and the responsible computer
131 incident response center.

133 (2) Isolated and contained to minimize damage and to preserve evidence that may be
134 required for damage assessment, risk assessment, law enforcement, or CI purposes. All affected
135 media is to be considered classified at the same level as the spilled information until the appropriate
136 remediation processes have been executed and verified.

138 (3) Verified to be classified by the information owner, who shall also ensure an
139 assessment is conducted, as appropriate, in accordance with References (d) and (f) and this Manual.

141 d. CNSS Instruction 1001 (Reference (bs)) implements Reference (br) and provides a list of
142 questions that should be asked when investigating a spill, potential options for remediating the
143 effects of a spill, and factors to be considered in selecting a remediation procedure.

145 e. Information concerning a classified spillage incident shall be protected from disclosure.
146 Communications regarding the fact that a spill situation exists should be communicated to those
147 involved, including the remediation teams, via secure communications whenever possible. The

148 technical remediation teams must be cleared to the level of the information that may have been
149 spilled.

150
151 f. Decisions regarding mitigation procedures, including disposition of affected media (i.e.,
152 sanitization, physical removal, or destruction) shall realistically consider the potential harm that
153 may result from compromise of spilled information.

154
155 g. During a spill event, a speedy and coordinated response among security, IA, and other
156 technical personnel is vital. Significant unauthorized or inadvertent dissemination of classified
157 information on unclassified information systems can occur rapidly.

158
159 (1) Once a spill is reported, the information system support organization must, whenever
160 possible, quickly implement technical isolation of contaminated workstations, servers, and back- up
161 systems to avoid spreading the contamination, to avoid loss of systems availability, and to
162 minimize exposure of classified information to those individuals or organizations not authorized to
163 receive it. At the same time, the security and IT staffs must begin the process of determining
164 whether a security incident has actually occurred. If so, remediation procedures, which must be
165 developed, approved, and tested in advance, should be implemented.

166
167 (2) E-mail (whether in the body of the e-mail or attachment) is the most common method
168 by which spills occur. The IA staff should have proven procedures to remediate up to Secret- level
169 spills to portable computing devices. Remediation of top secret, SAP, and SCI spills to PEDs
170 (personal or GFE)), however, may entail destruction of the hardware.

171
172 (3) For secret-level spills and below, the technical state of the art currently allows for
173 overwriting and sanitization of contaminated media, and reentry of the media into service. There is
174 no approved overwriting or sanitization procedure for media that has been contaminated with top
175 secret, SAP, or SCI data, short of physical destruction. However, such media may continue to be
176 used if (re)classified at the higher level, where appropriate.

177
178 (4) Early identification of classified spills, and a thorough understanding of where the
179 spilled data was sent, is essential to avoid widespread contamination (or re-contamination) of back-
180 up servers, tape systems, and off-site storage locations, most of which are configured to run nightly
181 or during periods of low usage.

182
183 h. Classified spills to a personally owned device should also be reported to security officials
184 immediately so remediation can be undertaken as necessary to prevent further unauthorized
185 disclosure.

186 187 188 6. DISPOSAL OF COMPUTER MEDIA

189
190 a. NSA/CSS publishes lists of products that meet specific performance criteria for sanitizing,
191 destroying or disposing of various types of media containing sensitive or classified information.
192 Among the products identified are those that can be used for erasure of magnetic storage devices
193 (e.g., hard drives) and destruction of optical media (e.g., CDs and DVDs). The lists are available at
194 http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml or by calling (410) 854-
195 6358. The NSA/CSS Storage Device Declassification Manual, available at that web address,
196 addresses procedures required for sanitization, declassification and release of computer storage

197 devices that have held classified information. Overwriting as a method of clearing previously
198 classified data may be used when the media is reused within the same environment. Sections 17
199 and 18 of Enclosure 3 of this Volume provide additional guidance on destruction of classified
200 information.

201
202 b. When no longer needed, UNCLASSIFIED computer systems and hard drives may be
203 disposed of outside the DoD. In some circumstances, the equipment may be provided to non-
204 government entities for reutilization. To ensure that no data or information remains on operable
205 unclassified hard drives that are transferred or permanently removed from DoD custody, the drives
206 must be sanitized by overwriting. Where overwriting is inappropriate or cannot be accomplished
207 (e.g., inoperable disk) or the drives are to be totally removed from service (i.e., thrown away), the
208 drives must be destroyed. The specific methods and procedures differ depending on sensitivity of
209 data and ownership of the hard drive. To ensure DoD information is not inadvertently disclosed to
210 unauthorized individuals, the activity security manager should coordinate with the local AO and/or
211 IT staff to ensure local procedures for disposal of computer hard drives appropriately address
212 removal of U.S. Government data prior to disposal (See Assistant Secretary of Defense for
213 Command, Control, Communications and Intelligence Memorandum (Reference (bt)) for detailed
214 guidance).

215
216
217 7. NON-TRADITIONAL WORK ENVIRONMENTS. Increasingly, a wide variety of sensitive
218 and even classified activities are performed from non-traditional work environments, to include
219 employee homes. In the historic context, this work has principally involved unclassified
220 information and projects. However, classified IT (e.g., SIPRNET) systems and installations are
221 increasingly being approved for utilization by senior personnel. When such is the case, in addition
222 to the requirements of section 12 of Enclosure 2 of this Volume, the following minimum physical
223 and administrative security criteria must be addressed:

224
225 a. Physical site security survey/analysis. Where prudent, a crime survey may be requested
226 from local authorities to facilitate understanding of risks associated with the site.

227
228 b. Employee training on classified information systems operation, as well as protection and
229 storage of classified information and COMSEC materials.

230
231 c. Provisions for secure storage and/or destruction of any classified information that may be
232 required or generated (e.g. storage of COMSEC key materials, classified hard drives, and
233 documents).

234
235 d. Application of and compliance with requirements for security-in-depth.

236
237 e. Written approval for such use of classified information and equipment.

238
239
240 8. REQUIREMENT FOR ENCRYPTION OF CERTAIN UNCLASSIFIED DATA. In
241 accordance with DoD policy, all unclassified DoD data that has not been approved for public
242 release and is stored on mobile computing devices or removable storage media must be encrypted
243 using commercially available encryption technology. This requirement includes all CUI as well as
244 other unclassified information that has not been reviewed and approved for public release. See
245 ASD(NII) Memorandum (Reference (bu)) for detailed guidance.

246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294

9. PII

a. PII, which is a type of CUI, must be protected from public disclosure in accordance with Federal policy, as described in ASD(NII) Memorandum (Reference (bv)) and Director, Administration and Management Memorandum (Reference (bw)). Some PII also qualifies for protection under the provisions of section 552a of Reference (bk) (also known and hereinafter referred to as “The Privacy Act of 1974, as amended”). Certain PII requires data-at-rest encryption and other protections.

b. PII has protection and reporting requirements of which the activity security manager should be aware in the event the loss or unauthorized disclosure of PII (known as a “breach”) is reported to the security office, separately or as part of an unauthorized disclosure of classified information. Although Privacy Act and/or IT officials are responsible for addressing a breach, activity security managers should be familiar with the protection and breach reporting requirements, the required timeframes for such reports, and the process identified in the DoD Component breach remediation plan for responding to breaches. A breach may trigger a chain of required actions, including notifications to the USCYBERCOM, United States Computer Emergency Readiness Team, the DoD Component Head, and DoD Privacy Act officials. Breach reports must be unclassified.

10. NEW TECHNOLOGY AND EQUIPMENT. Technology, in general, and IT technology specifically, changes much more quickly than information security policy. New products for data storage, communications, access control, and intrusion detection, and new IT equipment and peripherals (e.g., hand-held classified devices such as the Secure Mobile Environment PED (commonly referred to as “SME PED”)) all have implications, and potential challenges, for information security. The activity security manager must remember that the fundamental principles upon which the information security program resides are still applicable and provide the foundation for dealing with new capabilities. The activity security manager must work with the IAM and the local AO(s) to identify new risks and develop appropriate procedures to mitigate those risks. Where new policy or procedures are required to address new capabilities, suggested updates and/or issues should be forwarded through the security chain of command to the Director of Security, USD(I&S).

11. INTERNET-BASED SOCIAL NETWORKING SERVICES. Use of Internet-based social networking services, such as Facebook, Twitter, and YouTube is governed by DoDI 8170.01 (Reference (bx)). The policy addresses both official use of such capabilities and non-official use by DoD personnel. It also covers use of other publicly accessible information capabilities and applications available on the Internet (e.g., wikis, blogs) in locations not owned, operated, or controlled by the DoD or the Federal Government. As each DoD Component is responsible for ensuring all uses of these services are compliant with information security, IA and OPSEC policies and procedures, officials from these disciplines need to coordinate efforts to implement appropriate training, procedures, and oversight. The requirements for protecting classified information and CUI from unauthorized disclosure are the same when using social networking services as when using other media and methods of dissemination and the penalties for ignoring the requirements are likewise the same.

295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343

12. MARKING REQUIREMENTS FOR ELECTRONIC INFORMATION. Regardless of media, the requirement to identify as clearly as possible the information requiring protection remains. Where it is not feasible to include markings with all of the information required for classified documents, an explanatory statement that provides the required information shall be included on the item or with the documentation that accompanies it.

a. For specific guidance on marking in an electronic environment, see section 17, Enclosure 3 of Volume 2 of this Manual, as well as related information in section 16 (briefing slides) and paragraph 18.g (removable electronic storage media) of the same enclosure.

b. The use of metadata and other electronic tags, as required by DoDD 8320.02 (Reference (ca)), to identify the classification level, releasability, and other security attributes of electronic data files can facilitate automated application and enforcement of security measures. However, it is imperative that metadata and electronic tags associated with declassified or downgraded information in electronic format be reviewed and updated or deleted, as necessary, to reflect the actual classification and other attributes of the information. Precautions must be taken to ensure classified attributes are not released with unclassified data.

13. PROCESSING REQUIREMENTS FOR SPECIFIC TYPES OF INFORMATION

a. SCI. SCI, regardless of classification level, must be processed only on an information system accredited for SCI processing (e.g., Joint Worldwide Intelligence Communications System (JWICS)). It may not be processed on, transferred to, or stored on SIPRNET, even if the information is SECRET//SI, SECRET//HCS, etc., as SIPRNET is not accredited for SCI. Any transfer to and/or processing of SCI on SIPRNET constitutes a data spillage from a higher to a lower-security information domain, in accordance with Reference (br).

b. RD and Critical Nuclear Weapons Design Information (CNWDI). RD and CNWDI require certain access and dissemination controls, as specified by DoDI 5210.02 (Reference (bz)), beyond those for other information of a comparable level of security classification. Requirements for processing RD or CNWDI are specified in section 12, Enclosure 3 of Volume 1 of this Manual.

c. SAP. SAP information, regardless of classification, shall be processed only on an information system specifically accredited for SAP processing and operating at a classification level that meets or exceeds the classification level of the SAP data.

d. Controlled Imagery. Information marked "IMCON" (controlled imagery) may not be processed on SIPRNET or posted to SIPRNET websites without prior approval from the National Geospatial-Intelligence Agency. See Appendix 2, Enclosure 4 of Volume 2 of this Manual.

e. NATO Information. NATO information, regardless of classification, must be processed on U.S. government CLASSIFIED information systems operating at an appropriate level of classification with encrypted data transport and storage and specifically accredited for NATO processing, in accordance with the requirements of Reference (ab) and Deputy Secretary of Defense Memorandum (Reference (ca)). For further guidance on accreditation, handling and processing of NATO information, including how to handle data spills involving NATO information, contact the Central U.S. Registry.

344
345 f. CUI. CUI may NOT be posted to publicly-accessible Internet sites and may NOT be
346 posted to sites whose access is controlled only by domain (e.g., limited to .mil and/or .gov) as such
347 restricted access can easily be circumvented. At a minimum, posting CUI to a website requires
348 certificate-based (e.g., common access card) or password and ID access as well as encrypted
349 transmission using hypertext transfer protocol secure (https) or similar technology. CUI may also
350 have additional posting restrictions. See Deputy Secretary of Defense Memorandum (Reference
351 (cb)) for detailed guidance.

352
353
354 14. COMPILATION AND DATA AGGREGATION. The ability to create large databases as well
355 as nearly universal Internet posting of information makes use of search, data mining, and other data
356 correlation tools convenient and easy. All of these capabilities facilitate creation of classified
357 compilations of data. The activity security manager should consider the potential for creation of
358 classified compilations when reviewing Internet postings, new IT systems, and security
359 classification guides, and, as appropriate, when other classification assistance is requested. See
360 Enclosure 4 of Volume 1 of this Manual, for guidance on classification by or as a result of
361 compilation and Enclosure 6 of Volume 1 for considerations relative to Internet posting of data
362 elements known to comprise classified compilations.

GLOSSARYPART I. ABBREVIATIONS AND ACRONYMS

ACCM	alternative compensatory control measures
AECS	automated entry control systems
AO	Authorizing Official
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
AUS	Australia
A&A	Assessment and Authorization
CD	compact disc
CFR	Code of Federal Regulations
CI	counterintelligence
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CNSS	Committee on National Security Systems
CNWDI	critical nuclear weapon design information
COMSEC	communication security
CONUS	continental United States
CPI	critical program information
CUI	controlled unclassified information
DC	direct current
DCIO	defense criminal investigative organization
DCS	Defense Courier Service
DD	DoD
DGR	designated government representative
DMS	Defense Message System
DNI	Director of National Intelligence
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
DOE	Department of Energy
DOJ	Department of Justice
DSA	designated security authority
DUSD(I&S)	Deputy Under Secretary of Defense for Intelligence and Security
DVD	digital video disc (also digital versatile disc)
E.O.	Executive Order
FED-STD	Federal Standard
FLDCOM	Field Command
FGI	foreign government information
FMS	foreign military sales
FRD	Formerly Restricted Data
GAO	Government Accountability Office
GC, DoD	General Counsel of the Department of Defense
GPO	Government Printing Office
GSA	General Services Administration

HUMINT	human intelligence
IA	information assurance
IT AO	information technology authorizing official
IAM	information assurance manager
IAO	information assurance officer
ID	identification
IDE	intrusion detection equipment
IDS	intrusion detection system
IS	Information System
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
IT	information technology
JPAS	Joint Personnel Adjudication System
JWICS	Joint Worldwide Intelligence Communications System
LOA	Letter of Offer and Acceptance
MFR	Memorandum for Record
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NCIX	National Counterintelligence Executive
NDA	non-disclosure agreement
NOFORN	not releasable to foreign nationals
NTISSI	National Telecommunications Information Systems Security
OCA	original classification authority
ODNI	Office of the Director of National Intelligence
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence &
OUSD(P)	Office of the Under Secretary of Defense for Policy
PCU	premise control unit
PED	personal electronic device
PII	personally identifiable information
PIN	personal identification number
POE	port of embarkation
RD	Restricted Data
REL TO	authorized for release to
SAO	Senior Agency Official
SAP	special access program
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SF	standard form
SIPRNET	Secret Internet Protocol Router Network
SPECAT	Special Category
TSA	Transportation Security Administration
TSCM	technical surveillance countermeasures
UK	United Kingdom
UL	Underwriters Laboratories
USC	United States Code
USCYBERCOM	U.S. Cyber Command
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy

369
370***(Added)(DAF) PART IA. ACRONYMS**

371

AA	Administrative Assistant
AF	Air Force
AFI	Air Force Instruction
AFPD	Air Force Publication Document
AFRIMS	Air Force Records Information Management System
ATOMAL	Atomic Information
CC	commander
CD	deputy commander
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
DAF	Department of the Air Force
DAFI	Department of the Air Force Instruction
DAFMAN	Department of the Air Force Manual
DAFPD	Department of the Air Force Policy Directive
DISS	Defense Information Security System
DRU	Direct Reporting Unit
DTS	Defense Travel System
EPL	evaluated products list
FLDCOM	Field Command
FOA	Field Operating Agency
IG	Inspector General
IP	information protection
MAJCOM	Major Command
NSA/CSS	National Security Agency/ Central Security Service
OF	Optional Form
OPR	office of primary responsibility
OSI	Office of Special Investigations
OCONUS	outside [the] continental United States
PED	portable electronic devices
PSO	program security officer
SAF	Secretary Air Force
SA	security assistance
SCG	security classification guide
SAMM	Security Assistance Management Manual
SC	security cooperation
SPE	security program executive
SSO	special security officer
USG	United States Government
UD	unauthorized disclosure
USSF	United States Space Force

372
373
374
375
376
377
378
379

PART II. DEFINITIONS

380
381 Unless otherwise noted, these terms and their definitions are for the purpose of this Manual.

382
383 access. The ability or opportunity to obtain knowledge of classified information.

384
385 activity head. See “heads of DoD activities.”

386
387 activity security manager. The individual specifically designated in writing and responsible for the
388 activity’s information security program which ensures that classified information and CUI is
389 properly handled during its entire life cycle. This includes ensuring it is appropriately identified,
390 marked, stored, disseminated, disposed of, and accounted for, as well as providing guidance on the
391 handling of security incidents to minimize adverse effects and ensure that appropriate corrective
392 action is taken. The security manager may be assigned responsibilities in other security disciplines
393 such as personnel and physical security, etc.

394
395 agency. Any “Executive Agency” as defined in section 105 of Reference (bm); any “Military
396 Department” as defined in section 102 of Reference (bm); and any other entity within the Executive
397 Branch that comes into the possession of classified information.

398
399 alarmed zone. The totality of area covered by a premise control unit and the sensors it serves.

400
401 Australian Communities. The Australian Government entities with facilities and non-
402 governmental facilities identified on the Department of State’s Directorate of Defense Trade
403 Controls website (<http://www.pmdtc.state.gov/treaties/index.html>) at the time of export.

404
405 authentication. Those measures designed to establish the validity of attributes associated with some
406 entity (e.g., user, process, or device), or a means of verifying an individual’s authorization to
407 receive specific categories of information. Authentication is often accomplished as a prerequisite to
408 allowing access to resources in an information system.

409
410 authorized person. A person who has a favorable determination of eligibility for access to
411 classified information, has signed a SF 312, and has a need to know for the specific classified
412 information in the performance of official duties.

413
414 automated information system. An assembly of computer hardware, software, or firmware
415 configured to collect, create, communicate, compute, disseminate, process, store, or control data or
416 information.

417
418 automatic declassification. The declassification of information based solely upon:

- 419
- 420 • The occurrence of a specific date or event as determined by the OCA; or
 - 421 • The expiration of a maximum time frame for duration of classification established pursuant
422 to Reference (d).

423
424 availability. Timely, reliable access to data and information services for authorized users.

425
426 classification. The act or process by which information is determined to be classified information.

427
428 classified national security information. Information that has been determined pursuant to

429 Reference (d), or any predecessor order, to require protection against unauthorized disclosure and is
 430 marked to indicate its classified status when in documentary form.

431
 432 classifier. An individual who makes a classification determination and applies a security
 433 classification to information or material. A classifier may be an OCA or a person who derivatively
 434 assigned a security classification based on a properly classified source or a security classification
 435 guide.

436
 437 collateral information. All national security information classified Confidential, Secret, or Top
 438 Secret under the provisions of an E.O. for which special systems of compartmentation (such as SCI
 439 or SAP) are not formally required.

440
 441 COMSEC. The protection resulting from all measures designed to deny unauthorized persons
 442 information of value that might be derived from the possession and study of telecommunications
 443 and to ensure the authenticity of such communications. COMSEC includes crypto security,
 444 emission security, transmission security, and physical security of COMSEC material and
 445 information.

446
 447 compromise. An unauthorized disclosure of classified information.

448
 449 confidentiality. Assurance that information is not disclosed to individuals, devices, processes, or
 450 other entities unless they have been authorized access to the information.

451
 452 CONUS. U.S. territory, including adjacent territorial waters, located within the North American
 453 content between Canada and Mexico.

454
 455 CPI. Defined in DoDI 5200.39 (Reference (ce)).

456
 457 AO. The official with the authority to formally assume responsibility for operating a system at an
 458 acceptable level of risk. This term is synonymous with designated accrediting authority and
 459 delegated accrediting authority.

460
 461 damage assessment. A formal multi-disciplinary analysis to determine the effect of a compromise
 462 of classified information on the national security

463
 464 damage to the national security. Harm to the national defense or foreign relations of the United
 465 States from the unauthorized disclosure of information, taking into consideration such aspects of
 466 the information as the sensitivity, value, utility, and provenance of that information.

467
 468 declassification. The authorized change in the status of information from classified information to
 469 unclassified information.

470
 471 declassification authority

472
 473 • The official who authorized the original classification, if that official is still serving in the
 474 same position;
 475 • The originator's current successor in function; A supervisory official of either; or
 476 • Officials delegated declassification authority in writing by the agency head or the senior
 477 agency official.

478
 479 declassification guide. Written instructions issued by a declassification authority that describes the
 480 elements of information regarding a specific subject that may be declassified and the elements that
 481 must remain classified. Also a guide providing classification and declassification instructions
 482 specifically for information that is 25 years old or older and of permanent historical value. A
 483 declassification guide is the most commonly used vehicle for obtaining ISCAP approval of 25-year
 484 exemptions from the automatic declassification provisions of Reference (d).

485
 486 defense articles. For purposes of the Defense Trade Cooperation Treaty between the United States
 487 and Australia or the United Kingdom, those articles, services, and related technical data, including
 488 software, in tangible or intangible form, listed on the United States Munitions List of Reference (y).
 489 Defense articles exempt from the scope of section 126.17 of Reference (y) are identified in
 490 Supplement No. 1 to Part 126 of Reference.

491
 492 derivative classification. Incorporating, paraphrasing, restating, or generating in new form
 493 information that is already classified, and marking the newly developed material consistent with the
 494 classification markings that apply to the source information. Includes the classification of
 495 information based on classification guidance. The duplication or reproduction of existing classified
 496 information is not derivative classification.

497
 498 distribution statement. A statement used on a technical document to denote the extent of its
 499 availability for secondary distribution, release, and disclosure without additional approvals or
 500 authorizations. A distribution statement marking is distinct from and in addition to a security
 501 classification marking. A distribution statement is also required on security classification guides
 502 submitted to DTIC.

503
 504 document. Any recorded information, regardless of the nature of the medium or the method or
 505 circumstances of recording. This includes any physical medium in or on which information is
 506 recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic
 507 storage media.

508
 509 downgrading. A determination by a declassification authority that information classified and
 510 safeguarded at a specified level shall be classified and safeguarded at a lower level.

511
 512 escort. A cleared individual who accompanies a shipment of classified material to its destination.
 513 The classified material does not remain in the personal possession of the escort, but the conveyance
 514 in which the material is transported remains under the constant observation and control of the
 515 escort.

516
 517 espionage. Those activities designed to obtain, deliver, communicate, or transmit information
 518 relating to the national defense with the intent or reason to believe such information will be used to
 519 the injury of the U.S. or to the advantage of a foreign nation or transnational entity.

520
 521 exempted. Nomenclature and marking indicating information has been determined to fall within an
 522 enumerated exemption from automatic declassification in accordance with Reference (d).

523
 524 FGI

525
 526 • Information provided to the U.S. Government by a foreign government or governments, an

527 international organization of governments, or any element thereof, with the expectation that
528 the information, the source of the information, or both, are to be held in confidence.

- 529 • Information produced by the U.S. Government pursuant to or as a result of a joint
530 arrangement with a foreign government or governments, or an international organization of
531 governments, or any element thereof, requiring that the information, the arrangement, or
532 both, are to held in confidence.
- 533 • Information received and treated as “Foreign Government Information” pursuant to the
534 terms of a predecessor order to Reference (d).

535
536 FRD. Information removed from the Restricted Data category upon a joint determination by the
537 Department of Energy (or antecedent agencies) and the Department of Defense that such
538 information relates primarily to the military utilization of atomic weapons and that such
539 information can be safeguarded adequately as classified defense information. For purposes of
540 foreign dissemination, this information is treated in the same manner as Restricted Data.

541
542 ***(Added)(DAF) Foreign Military Sales (FMS). That portion of United States security**
543 **assistance for sales programs that require agreements/contracts between the United States**
544 **Government and an authorized recipient government or international organization for**
545 **defense articles and services to be provided to the recipient for current stocks or new**
546 **procurements under Department of Defense-managed contracts, regardless of the source of**
547 **financing.**

548
549 heads of DoD activities. Heads, either military or civilian, of organizations, commands, and staff
550 elements subordinate to a DoD Component, with jurisdiction over and responsibility for the
551 execution of the organization’s mission and functions, including its information security program.
552 The official may variously carry the title of commander, commanding officer, or director, or other
553 equivalent title.

554
555 homeland. The physical region that includes the continental U.S., Alaska, Hawaii, U.S.
556 possessions and territories, and surrounding territorial waters and airspace.

557
558 information. Any knowledge that can be communicated or documentary material, regardless of its
559 physical form or characteristics, which is owned by, produced by or for, or is under the control of
560 the U.S. Government.

561
562 information security. The system of policies, procedures, and requirements established in
563 accordance with Reference (d) to protect information that, if subjected to unauthorized disclosure,
564 could reasonably be expected to cause damage to national security. The term also applies to
565 policies, procedures and requirements established to protect controlled unclassified information,
566 which may be withheld from release to the public in accordance with statute, regulation, or policy.

567
568 infraction. Any knowing, willful, or negligent action contrary to the requirements of Reference (d),
569 its implementing directives, or this Manual that does not constitute a “violation,” as defined herein.

570
571 inquiry. The initial fact-finding and analysis process to determine the facts of any security incident.

572
573 integrity. The state that exists when information is unchanged from its source and has not been
574 accidentally or intentionally modified, altered, or destroyed. Integrity in the IA environment
575 addresses the logical correctness, completeness, and reliability of the operating system, and the

576 system hardware, software and data. In a formal security mode, integrity is interpreted more
577 narrowly to mean protection against unauthorized modification or destruction of data or
578 information.

579

580 Intelligence Community. An element or agency of the U.S. Government identified in or designated
581 pursuant to section 3(4) of the National Security Act of 1947, as amended (Reference (ce)), or
582 section 3.5(h) of E.O. 12333 (Reference (cf)).

583

584 international program. Any program, project, contract, operation, exercise, training, experiment, or
585 other initiative that involves a DoD Component or a DoD contractor and a foreign government,
586 international organization, or corporation that is located and incorporated to do business in a
587 foreign country.

588

589 investigation. An in-depth, comprehensive examination of the facts associated with a security
590 violation.

591

592 loss. The inability to physically locate or account for classified information.

593

594 material. Any product or substance on or in which information is embodied.

595

596 metadata. Structured information that describes, explains or locates data or otherwise makes data
597 easier to retrieve, use or manage. Metadata captures or specifies basic attributes and characteristics
598 about information and is often referred to as information about information.

599 Typical metadata in an electronic environment includes such attributes as author, creation date, file
600 size, and storage location. Security metadata may include attributes such as classification level,
601 OCA, and date for declassification.

602

603 national security. The national defense or foreign relations of the U.S. National security includes
604 defense against transnational terrorism.

605

606 need-to-know. A determination made by an authorized holder of classified information that a
607 prospective recipient requires access to specific classified information in order to perform or assist
608 in a lawful and authorized governmental function.

609

610 ***(Added)(DAF) negligent. An incident is negligent if the person acted unreasonably in**
611 **causing a security incident or unauthorized disclosure (e.g., a careless lack of attention to**
612 **detail, or reckless disregard for proper procedures).**

613

614 network. A system of two or more computers that can exchange data or information.

615

616 nickname. A nickname is a combination of two separate unclassified words that is assigned an
617 unclassified meaning and is employed only for unclassified administrative, morale, or public
618 information purposes.

619

620 non-repudiation. The condition where the sender of data is provided with proof of delivery and the
621 recipient is provided with proof of the sender's identity, so neither can later deny having processed
622 the data.

623

624 open storage area. An area constructed in accordance with the requirements of the Appendix to

625 Enclosure 3 of this Volume and authorized by the senior agency official for open storage of
626 classified information.

627
628 original classification. An initial determination that information requires, in the interests of
629 national security, protection against unauthorized disclosure.

630
631 OCA. An individual authorized in writing, either by the President, the Vice President, or by agency
632 heads or other officials designated by the President, to originally classify information (i.e., to
633 classify information in the first instance).

634
635 permanent historical value. Having sufficient value to warrant being maintained and preserved
636 permanently.

637
638 PII. Unique information about an individual that can be used to distinguish or trace his or her
639 identity. It includes, but is not limited to, name, social security number, date and place of birth,
640 mother's maiden name, home address and phone number, personal e-mail address, biometric
641 records, financial transactions, medical history, criminal or employment history, and other
642 information to which a security manager may have access. PII does not include an individual's
643 name when it is associated with work elements, such as duty phone number, duty address, and
644 U.S. Government e-mail address.

645
646 protective security service. Defined in DoD 5220.22-M (Reference (w)).

647
648 public media. A medium of communications designed to reach the public. Public media includes
649 print media (e.g., newspapers, magazines, books), broadcast media (e.g., radio, television) and
650 Internet media (e.g., websites, blogs, tweets).

651
652 records. The records of an agency and Presidential papers or Presidential records, as those terms
653 are defined in chapters 22 and 33 of Reference (t), including those created or maintained by a
654 U.S. Government contractor, licensee, certificate holder, or grantee that are subject to the
655 sponsoring agency's control under the terms of the contract, license, certificate, or grant.

656
657 records management. The planning, controlling, directing, organizing, training, promoting, and
658 other managerial activities involved with respect to records creation, records maintenance and use,
659 and records disposition in order to achieve adequate and proper documentation of the policies and
660 transactions of the Federal Government and effective and economical management of agency
661 operations. Within the DoD, records management is implemented by Reference (u).

662
663 RD. All data concerning design, manufacture, or utilization of atomic weapons; the production of
664 special nuclear material; or the use of special nuclear material in the production of energy, but not
665 data declassified or removed from the Restricted Data category pursuant to section 2162 of The
666 Atomic Energy Act of 1954, as amended (Reference (cg)).

667
668 safeguarding. Measures and controls that are prescribed to protect classified information.

669
670 SAP. A program established for a specific class of classified information that imposes
671 safeguarding and access requirements that exceed those normally required for information at the
672 same classification level. In the DoD, any DoD program or activity (as authorized in Reference
673 (d)), employing enhanced security measures (e.g., safeguarding, access requirements, etc.),

674 exceeding those normally required for collateral information at the same level of classification,
675 shall be established, approved, and managed as a DoD SAP in accordance with Reference (ag).
676

677 SCI. Classified information concerning or derived from intelligence sources, methods, or
678 analytical processes that is required to be handled within formal access control systems established
679 by the Director of National Intelligence.
680

681 secure room. An open storage area.
682

683 security classification guide. A documentary form of classification guidance issued by an OCA
684 that identifies the elements of information regarding a specific subject that must be classified and
685 establishes the level and duration of classification for each such element.
686

687 security clearance eligibility. A determination that a person is eligible in accordance with the
688 standards of Reference (I) for access to classified information.
689

690 ***(Added)(DAF) security cooperation. All Department of Defense interactions with foreign**
691 **security establishments to build security relationships that promote specific United States**
692 **security interests, develop allied and partner nation military and security capabilities for self-**
693 **defense and multinational operations, and provide United States forces with peacetime and**
694 **contingency access to allied and partner nations.**
695

696 security-in-depth. A determination by the senior agency official that a facility's security program
697 consists of layered and complementary security controls sufficient to deter and detect unauthorized
698 entry and movement within the facility. Examples include, but are not limited to, use of perimeter
699 fences, employee and visitor access controls, use of an IDS, random guard patrols throughout the
700 facility during non-working hours, closed circuit video monitoring or other safeguards that mitigate
701 the vulnerability of open storage areas without alarms and security containers during non-working
702 hours.
703

704 self-inspection. The internal review and evaluation of individual DoD Component activities and
705 the DoD Component as a whole with respect to the implementation of the program established in
706 accordance with References (b), (d), and (f), and this Manual.
707

708 senior agency official. An official appointed by the Head of a DoD Component to be responsible
709 for direction, administration, and oversight of the Component's Information Security Program, to
710 include classification, declassification, safeguarding, and security education and training programs,
711 and for the efficient and effective implementation of References (b), (d), (e), and (f) and the
712 guidance in this Manual. Where used in reference to authorities under section 5.4(d) of Reference
713 (d), this term applies only to the Senior Agency Officials of the Military Departments and of the
714 DoD.
715

716 telecommunications. The preparation, transmission, or communication of information by
717 electronic means.
718

719 unauthorized disclosure. Communication or physical transfer of classified or controlled
720 unclassified information to an unauthorized recipient.
721

722 United Kingdom communities. The UK Government entities with facilities and non- governmental

723 facilities identified on the Department of State's Directorate of Defense Trade Controls website
724 (<http://www.pmddtc.state.gov/treaties/index.html>) at the time of export.

725
726 United States and its territories. The 50 states, the District of Columbia, Puerto Rico, Guam,
727 American Samoa, the United States Virgin Islands, Wake Island, Johnston Atoll, Kingman Reef,
728 Palmyra Atoll, Baker Island, Howland Island, Jarvis Island, Midway Islands, Navassa Island, and
729 Northern Mariana Islands.

730
731 vault. An area approved by the Head of the DoD Component which is designed and constructed of
732 masonry units or steel lined construction to provide protection against forced entry and which is
733 equipped with a GSA-approved vault door and lock. A modular vault approved by the GSA may
734 be used in lieu of a vault.

735
736 violation

- 737
- 738 • Any knowing, willful, or negligent action that could reasonably be expected to result in an
739 unauthorized disclosure of classified information;
 - 740 • Any knowing, willful, or negligent action to classify or continue the classification of
741 information contrary to the requirements of Reference (d), its implementing directives, or
742 this Manual; or
 - 743 • Any knowing, willful, or negligent action to create or continue a special access program
744 contrary to the requirements of Reference (d), Reference (ah), or this Manual.

745
746 ***(Added)(DAF) willful. An incident is willful if the person purposefully disregards DoD or
747 Air Force security or information safeguarding policies or requirements (e.g., intentionally
748 bypassing a known security control).**

749
750 **(Added)(DAF) zeroize. Practice of erasing sensitive parameters from a cryptographic module
751 to prevent their disclosure if the equipment is captured. This is generally accomplished by
752 altering or deleting the contents to prevent recovery of the data.**