



NATIONAL INDUSTRIAL SECURITY PROGRAM

OPERATING MANUAL

**February 2006
Incorporating Change 1
March 28, 2013**

**With inline ISLs:
ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06; 2014-01,
-02, and -03**

Compiled May 2, 2014

May 2, 2014

This compilation, like the May 10, 2010 compilation, is provided as an aide.

This compiled NISPOM with ISLs in *blue* is an unofficial reference document.

The official NISPOM is Change 1, dated March 28, 2013; and the individual ISLs can be found at http://www.dss.mil/isp/fac_clear/download_nispom.html.

TABLE OF CONTENTS

	Page
Table of Contents	1
References	14
AL1. Acronyms	16

CHAPTER 1. GENERAL PROVISIONS AND REQUIREMENTS

Section 1. Introduction	
1-100. Purpose	1-1-1
1-101. Authority	1-1-1
1-102. Scope	1-1-2
ISL 2006-01 #1 (1-102)	
1-103. Agency Agreements	1-1-2
ISL 2012-01 (1-103.b.)	
ISL 2013-02 (1-103.b.)	
ISL 2013-04 (1-103.b.)	
ISL 2014-02 (1-103.b.)	
1-104. Security Cognizance	1-1-3
1-105. Composition of Manual	1-1-3
1-106. Manual Interpretations	1-1-3
1-107. Waivers and Exceptions to this Manual	1-1-4
Section 2. General Requirements	
1-200. General	1-2-1
ISL 2006-02 #1 (1-200)	
1-201. Facility Security Officer (FSO)	1-2-1
1-202. Standard Practice Procedures	1-2-1
1-203. One-Person Facilities	1-2-1
1-204. Cooperation with Federal Agencies and Officially Credentialed Representatives of Those Agencies	1-2-1
ISL 2006-01 #2 (1-204)	
ISL 2010-01 #1 (1-204)	
1-205. Security Training and Briefings	1-2-2
1-206. Security Reviews	1-2-2
ISL 2006-02 #2 (1-206)	
1-207. Hotlines	1-2-3
1-208. Classified Information Procedures Act (CIPA)	1-2-4
Section 3. Reporting Requirements	
1-300. General	1-3-1
1-301. Reports to be Submitted to the FBI	1-3-1
ISL 2010-02 (rescinded by ISL 2013-05)	
ISL 2013-05 (1-301)	
1-302. Reports to be Submitted to the CSA	1-3-2
ISL 2006-02 #3 (1-302)	
ISL 2006-02 #4 (1-302, 1-303, 1-304)	
ISL 2011-04 (1-302.a.)	

ISL 2009-03 (1-302.g.(5) and 2-302)	
1-303. Reports of Loss, Compromise, or Suspected Compromise	1-3-7
ISL 2006-02, #4 (1-302, 1-303, 1-304)	
ISL 2006-02 #5 (1-303 and 4-218)	
1-304. Individual Culpability Reports	1-3-8
ISL 2006-02 #4 (1-302, 1-303, 1-304)	

CHAPTER 2. SECURITY CLEARANCES

Section 1. Facility Clearances

2-100. General	2-1-1
2-101. Reciprocity	2-1-1
2-102. Eligibility Requirements	2-1-1
ISL 2006-02 #6 (2-102 and 7-101)	
ISL 2009-02 #1 (2-102)	
ISL 2013-01 (2-102.b.)	
2-103. Processing the FCL	2-1-2
2-104. PCLs Required in Connection with the FCL	2-1-2
2-105. PCLs Concurrent with the FCL	2-1-3
2-106. Exclusion Procedures	2-1-3
2-107. Interim FCLs	2-1-3
2-108. Multiple Facility Organizations (MFOs)	2-1-3
ISL 2006-02 #7 (2-108)	
2-109. Parent-Subsidiary Relationships	2-1-3
2-110. Termination of the FCL	2-1-3
2-111. Records Maintenance	2-1-4

Section 2. Personnel Security Clearances

2-200. General	2-2-1
ISL 2006-01 #3 (2-200)	
ISL 2006-01 #4 (2-200 and 2-211)	
ISL 2006-02 #8 (2-200)	
ISL 2010-01 #2 (2-200.b.)	
2-201. Investigative Requirements	2-2-2
ISL 2006-02 #9 (2-201)	
ISL 2006-02 #10 (2-201)	
2-202. Procedures for Completing the Electronic Version of the SF 86	2-2-3
ISL 2006-01 #5 (2-202)	
2-203. Common Adjudicative Standards	2-2-4
2-204. Reciprocity	2-2-4
2-205. Pre-employment Clearance Action	2-2-4
ISL 2009-02 #2 (2-205)	
2-206. Contractor-Granted Clearances	2-2-5
2-207. Verification of U.S. Citizenship	2-2-5
2-208. Acceptable Proof of Citizenship	2-2-5
ISL 2010-01 #3 (2-208)	
ISL 2011-02 #1 (2-208)	
2-209. Non-U.S. Citizens	2-2-6
2-210. Access Limitations of an LAA	2-2-6
ISL 2006-02 #11 (2-210)	
2-211. Interim PCLs	2-2-6

ISL 2006-01 #4 (2-200 and 2-211)	
2-212. Consultants	2-2-7
ISL 2006-02 #12 (2-212)	
Section 3. Foreign Ownership, Control, or Influence (FOCI)	
2-300. Policy	2-3-1
ISL 2009-02 #3 (2-300.c.)	
2-301. Factors	2-3-2
2-302. Procedures	2-3-2
ISL 2006-01 #6 (2-302)	
ISL 2009-03 (1-302.g.(5) and 2-302)	
2-303. FOCI Action Plans	2-3-3
ISL 2006-01 #7 (2-303)	
ISL 2011-02 #2 (2-303.c.(2))	
2-304. Citizenship of Persons Requiring PCLs	2-3-5
2-305. Qualifications of Trustees, Proxy Holders, and Outside Directors	2-3-5
2-306. GSC	2-3-5
2-307. TCP	2-3-6
2-308. Annual Review and Certification	2-3-6
2-309. Limited FCL	2-3-7
2-310. Foreign Mergers, Acquisitions and Takeovers and the Committee on Foreign Investment in the United States (CFIUS)	2-3-7

CHAPTER 3. SECURITY TRAINING AND BRIEFINGS

Section 1. Security Training and Briefings	
3-100. General	3-1-1
3-101. Training Materials	3-1-1
3-102. FSO Training	3-1-1
ISL 2010-01 #4 (rescinded by ISL 2012-03)	
ISL 2012-03 (3-102)	
3-103. Government-Provided Briefings	3-1-1
3-104. Temporary Help Suppliers	3-1-1
3-105. Classified Information Nondisclosure Agreement (SF 312)	3-1-1
ISL 2006-02 #13 (3-105)	
ISL 2006-02 #14 (3-105)	
3-106. Initial Security Briefings	3-1-2
3-107. Refresher Training	3-1-2
3-108. Debriefings	3-1-2

CHAPTER 4. CLASSIFICATION AND MARKING

Section 1. Classification	
ISL 2013-06 #1 (Chapter 4)	
4-100. General	4-1-1
4-101. Original Classification	4-1-1
4-102. Derivative Classification Responsibilities	4-1-1
ISL 2013-06 #2 (4-102.d.)	
4-103. Security Classification Guidance	4-1-2
4-104. Challenges to Classification	4-1-3

4-105. Contractor Developed Information.....	4-1-3
4-106. Classified Information Appearing in Public Media.....	4-1-3
4-107. Downgrading or Declassifying Classified Information.....	4-1-4
ISL 2006-01 #8 (4-107 and 4-216.a.)	
Section 2. Marking Requirements	
4-200. General.....	4-2-1
4-201. Marking Requirements for Information and Material.....	4-2-1
4-202. Identification Markings.....	4-2-1
4-203. Overall Markings.....	4-2-1
4-204. Page Markings.....	4-2-1
4-205. Component Markings.....	4-2-1
4-206. Portion Markings.....	4-2-1
4-207. Subject and Title Markings.....	4-2-2
4-208. Markings for Derivatively Classified Documents.....	4-2-2
ISL 2013-06 #3 (4-208)	
4-209. Documents Generated Under Previous E.O.s.....	4-2-3
4-210. Marking Special Types of Material.....	4-2-4
4-211. Marking Transmittal Documents.....	4-2-4
4-212. Marking Wholly Unclassified Material.....	4-2-5
4-213. Marking Compilations.....	4-2-5
4-214. Working Papers.....	4-2-5
4-215. Marking Miscellaneous Material.....	4-2-5
4-216. Marking Training Material.....	4-2-5
4-217. Downgrading or Declassification Actions.....	4-2-5
ISL 2006-01 #8 (4-107 and 4-2167.a.)	
4-218. Upgrading Action.....	4-2-6
ISL 2006-02 #5 (1-303 and 4-218)	
4-219. Inadvertent Release.....	4-2-6
4-220. Marking requirements for transfers of defense articles to the United Kingdom.....	4-2-7
4-221. Comingling of Restricted Data and Formerly Restricted Data.....	4-2-7

CHAPTER 5. SAFEGUARDING CLASSIFIED INFORMATION

Section 1. General Safeguarding Requirements	
5-100. General.....	5-1-1
5-101. Safeguarding Oral Discussions.....	5-1-1
5-102. End of Day Security Checks.....	5-1-1
5-103. Perimeter Controls.....	5-1-1
5-104. Emergency Procedures.....	5-1-1
Section 2. Control and Accountability	
5-200. Policy.....	5-2-1
ISL 2006-01 #9 (5-200)	
5-201. Accountability for TOP SECRET.....	5-2-1
5-202. Receiving Classified Material.....	5-2-1
ISL 2006-01 #10 (5-202)	
ISL 2006-01 #11 (5-202 and 5-401)	
5-203. Generation of Classified Material.....	5-2-2
Section 3. Storage and Storage Equipment	
5-300. General.....	5-3-1

5-301. GSA Storage Equipment.....	5-3-1
ISL 2012-04 #1 (5-301)	
ISL 2014-03 #1 (5-301)	
5-302. TOP SECRET Storage.....	5-3-1
5-303. SECRET Storage.....	5-3-1
ISL 2011-01 (rescinded by ISL 2012-04 #2)	
ISL 2012-04 #2 (5-303)	
5-304. CONFIDENTIAL Storage.....	5-3-2
5-305. Restricted Areas.....	5-3-2
5-306. Closed Areas.....	5-3-2
ISL 2006-01 #12 (5-306)	
ISL 2006-01 #13 (5-306)	
ISL 2006-02 #16 (rescinded by ISL 2012-04 #3)	
ISL 2007-01 #1 (5-306, 8-100.b.)	
ISL 2006-02 #15 (5-306.a.)	
ISL 2012-04 #3 (5-306.b.)	
5-307. Supplemental Protection.....	5-3-5
5-308. Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas.....	5-3-5
5-309. Changing Combinations.....	5-3-5
ISL 2006-02 #17 (5-309.b.)	
5-310. Supervision of Keys and Padlocks.....	5-3-5
5-311. Repair of Approved Containers.....	5-3-6
ISL 2006-01 #14 (5-311)	
5-312. Supplanting Access Control Systems or Devices.....	5-3-6
5-313. Automated Access Control Systems.....	5-3-6
5-314. Electronic, Mechanical, or Electro-mechanical Devices.....	5-3-7
Section 4. Transmission	
5-400. General.....	5-4-1
5-401. Preparation and Receipting.....	5-4-1
ISL 2006-01 #11 (5-202 and 5-401)	
5-402. TOP SECRET Transmission Outside a Facility.....	5-4-1
5-403. SECRET Transmission Outside a Facility.....	5-4-1
ISL 2014-01 (5-403e and 5-404))	
5-404. CONFIDENTIAL Transmission Outside a Facility.....	5-4-3
5-405. Transmission Outside the United States and Its Territorial Areas.....	5-4-3
5-406. Addressing Classified Material.....	5-4-3
5-407. Transmission Within a Facility.....	5-4-3
5-408. SECRET Transmission by Commercial Carrier.....	5-4-3
ISL 2006-02 #18 (5-408 and 5-409) (rescinded by ISL 2014-01)	
5-409. CONFIDENTIAL Transmission by Commercial Carrier.....	5-4-4
5-410. Use of Couriers, Handcarriers, and Escorts.....	5-4-5
5-411. Use of Commercial Passenger Aircraft for Transmitting Classified Material.....	5-4-5
5-412. Use of Escorts for Classified Shipments.....	5-4-5
ISL 2006-01 #15 (5-412 and 10-402)	
5-413. Functions of an Escort.....	5-4-6
Section 5. Disclosure	
5-500. General.....	5-5-1
5-501. Disclosure to Employees.....	5-5-1
5-502. Disclosure to Subcontractors.....	5-5-1

5-503. Disclosure between Parent and Subsidiaries	5-5-1
ISL 2011-03 (5-503)	
5-504. Disclosure in an MFO	5-5-1
5-505. Disclosure to DoD Activities	5-5-1
5-506. Disclosure to Federal Agencies	5-5-1
5-507. Disclosure of Classified Information to Foreign Persons	5-5-1
5-508. Disclosure of Export Controlled Information to Foreign Persons	5-5-2
5-509. Disclosure to Other Contractors	5-5-2
5-510. Disclosure of Classified Information in Connection with Litigation	5-5-2
5-511. Disclosure to the Public	5-5-2
Section 6. Reproduction	
5-600. General	5-6-1
5-601. Limitations	5-6-1
5-602. Marking Reproductions	5-6-1
5-603. Records	5-6-1
Section 7. Disposition and Retention	
5-700. General	5-7-1
5-701. Retention of Classified Material	5-7-1
5-702. Termination of Security Agreement	5-7-1
5-703. Disposition of Classified Material Not Received Under a Specific Contract	5-7-1
5-704. Destruction	5-7-2
ISL 2007-01 #54 (5-704, 5-705, 8-103.f., 8-301)	
5-705. Methods of Destruction	5-7-2
5-706. Witness to Destruction	5-7-2
5-707. Destruction Records	5-7-2
5-708. Classified Waste	5-7-2
Section 8. Construction Requirements	
5-800. General	5-8-1
5-801. Construction Requirements for Closed Areas	5-8-1
5-802. Construction Requirements for Vaults	5-8-2
Section 9. Intrusion Detection Systems	
5-900. General	5-9-1
5-901. CSA Approval	5-9-1
ISL 2014-03 #2 (5-901)	
5-902. Central Monitoring Station	5-9-1
ISL 2006-02 #19 (5-902)	
ISL 2014-03 #3 (5-902)	
5-903. Investigative Response to Alarms	5-9-2
5-904. Installation	5-9-3
5-905. Certification of Compliance	5-9-3
5-906. Exceptional Cases	5-9-3

CHAPTER 6. VISITS and MEETINGS

Section 1. Visits	
6-100. General	6-1-1
6-101. Classified Visits	6-1-1
6-102. Need-to-Know Determination	6-1-1
6-103. Visits by Government Representatives	6-1-1
6-104. Visit Authorization	6-1-1

ISL 2006-01 #16 (6-104)	
ISL 2006-02 #20 (6-104)	
ISL 2010-01 #5 (6-104.a.)	
6-105. Long-Term Visitors	6-1-2
Section 2. Meetings	
6-200. General	6-2-1
6-201. Government Sponsorship of Meetings	6-2-1
6-202. Disclosure Authority at Meetings	6-2-2
6-203. Requests to Attend Classified Meetings	6-2-2

CHAPTER 7. SUBCONTRACTING

Section 1. Prime Contractor Responsibilities	
7-100. General	7-1-1
7-101. Responsibilities	7-1-1
ISL 2006-02 #6 (2-102 and 7-101)	
7-102. Security Classification Guidance	7-1-2
7-103. Responsibilities (Completion of the Subcontract)	7-1-2
7-104. Notification of Unsatisfactory Conditions	7-1-2

CHAPTER 8. INFORMATION SYSTEM SECURITY

Section 1. Responsibilities and Duties	
8-100. General	8-1-1
ISL 2007-01 #2 (8-100.a., 8-400)	
ISL 2007-01 #1 (5-306, 8-100.b.)	
ISL 2007-01 #33 (8-400, 8-100.c.)	
8-101. Responsibilities	8-1-1
ISL 2009-01 #1 (8-101.a., 8-610.a.(1)(b)(3))	
ISL 2009-01 #2 (8-101.a., 8-202, Chapter 8 Section 6)	
ISL 2007-01 #3 (8-101.b.)	
ISL 2007-01 #4 (8-101.b., 8-103)	
ISL 2007-01 #5 (8-101.b.)	
8-102. Designated Accrediting/Approving Authority	8-1-3
ISL 2007-01 #6 (8-102)	
8-103. IS Security Manager (ISSM)	8-1-4
ISL 2007-01 #4 (8-101.b., 8-103)	
ISL 2007-01 #54 (5-704, 5-705, 8-103.f., 8-301)	
ISL 2007-01 #27 (8-305, 8-103.f.(5))	
8-104. Information System Security Officer(s) (ISSO)	8-1-5
ISL 2007-01 #7 (8-104.d., 8-614)	
ISL 2007-01 #8 (8-104.l., 8-303.g.)	
8-105. Users of IS	8-1-6
ISL 2007-01 #19 (8-105.a., 8-302.a.)	
Section 2. Certification and Accreditation	
8-200. Overview	8-2-1
8-201. Certification Process	8-2-1
ISL 2007-01 #9 (8-201, 8-610.a.)	
ISL 2007-01 #14 (8-201, 8-202)	

8-202. Accreditation.....	8-2-2
ISL 2007-01 #10 (8-202, 8-610)	
ISL 2009-01 #2(8-101.a., 8-202, Chapter 8 Section 6)	
ISL 2007-01 #11 (8-202.c., 8-202.d., 8-202.e., 8-202.f.)	
ISL 2007-01 #12 (8-202.g.), #13 (8-202.g.)	
ISL 2007-01 #15 (8-202.g.(3))	
Section 3. Common Requirements	
8-300. Introduction.....	8-3-1
8-301. Clearing and Sanitization.....	8-3-1
ISL 2007-01 #16 (8-301.a., 8-501)	
ISL 2007-01 #54 (5-704, 5-705, 8-103.f., 8-301)	
8-302. Examination of Hardware and Software.....	8-3-4
ISL 2007-01 #17 (8-302.a.)	
ISL 2007-01 #18 (8-302.a.)	
ISL 2007-01 #19 (8-105.a., 8-302.a.)	
ISL 2007-01 #20 (8-302.a.)	
ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)(c))	
8-303. Identification and Authentication Management.....	8-3-5
ISL 2007-01 #23 (8-303.c.)	
ISL 2007-01 #24 (8-303.c.)	
ISL 2007-01 #8 (8-104.l., 8-303.g.)	
ISL 2007-01 #22 (8-303.i.)	
ISL 2007-01 #25 (8-303.i.(3))	
8-304. Maintenance.....	8-3-7
ISL 2007-01 #26 (8-304.b.(4))	
8-305. Malicious Code.....	8-3-7
ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)(c))	
ISL 2007-01 #27 (8-305, 8-103.f.(5))	
8-306. Marking Hardware, Output, and Media.....	8-3-8
ISL 2007-01 #28 (8-306.a.), #29 (8-306.c.)	
ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)(c))	
8-307. Personnel Security.....	8-3-9
8-308. Physical Security.....	8-3-10
ISL 2007-01 #30 (8-308.a.)	
ISL 2007-01 #31 (8-308.b.)	
8-309. Protection of Media.....	8-3-10
ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)(c))	
8-310. Review of Output and Media.....	8-3-11
ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)(c))	
8-311. Configuration Management.....	8-3-11
ISL 2007-01 #32 (8-311)	
Section 4. Protection Measures	
8-400. Protection Profiles.....	8-4-1
ISL 2007-01 #2 (8-100.a., 8-400)	
ISL 2007-01 #33 (8-400, 8-100.c.)	
8-401. Level of Concern.....	8-4-1
ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)(c))	
8-402. Protection Level.....	8-4-2
8-403. Protection Profiles.....	8-4-2
Section 5. Special Categories	
8-500. Special Categories.....	8-5-1

ISL 2007-01 #34 (8-500, 8-503.b.)	
ISL 2007-01 #41 (8-602, 8-500)	
8-501. Single-user, Stand-alone Systems	8-5-1
ISL 2007-01 #35 (8-501)	
ISL 2007-01 #16 (8-301.a., 8-501)	
8-502. Periods Processing	8-5-2
ISL 2007-01 #36 (8-502)	
ISL 2007-01 #37 (8-502.e.)	
8-503. Pure Servers	8-5-3
ISL 2007-01 #34 (8-500, 8-503.b.)	
ISL 2007-01 #38 (8-503.b.)	
ISL 2007-01 #39 (8-503.b.)	
8-504. Tactical, Embedded, Data-Acquisition, and Special-Purpose Systems	8-5-4
ISL 2007-01 #40 (8-504)	
8-505. Systems with Group Authenticators	8-5-4
Section 6. Protection Requirements	
ISL 2009-01 #2 (8-101.a., 8-202, Chapter 8 Section 6)	
8-600. Introduction	8-6-1
8-601. Alternate Power Source (Power)	8-6-1
8-602. Audit Capability	8-6-1
ISL 2007-01 #41 (8-602, 8-500)	
ISL 2007-01 #42 (8-602)	
ISL 2007-01 #43 (8-602)	
ISL 2007-01 #44 (8-602.a.)	
ISL 2007-01 #45 (8-602.a.(1)(c))	
8-603. Backup and Restoration of Data (Backup)	8-6-3
8-604. Changes to data (Integrity)	8-6-4
8-605. Data Transmission (Trans)	8-6-4
8-606. Access Controls (Access)	8-6-4
8-607. Identification and Authentication (I&A)	8-6-5
ISL 2007-01 #46 (8-607.b.(f))	
ISL 2007-01 #47 (8-607.c.)	
8-608. Resource Control (ResrcCtrl)	8-6-6
8-609. Session Controls (SessCtrl)	8-6-6
ISL 2007-01 #48 (8-609.b.(2))	
8-610. Security Documentation (Doc)	8-6-7
ISL 2007-01 #10 (8-202, 8-610)	
ISL 2007-01, #9 (8-201, 8-610.a.)	
ISL 2009-01 #1 (8-101.a., 8-610.a.(1)(b)3)	
ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-110.a. & b., 8-401, 8-610.a.(1)(c))	
8-611. Separation of Function Requirements (Separation)	8-6-9
8-612. System Recovery (SR)	8-6-9
8-613. System Assurance (SysAssur)	8-6-9
8-614. Security Testing (Test)	8-6-10
ISL 2007-01 #7 (8-104.d., 8-614)	
ISL 2007-01 #49 (8-614.a.)	
8-615. Disaster Recovery Planning	8-6-10
Section 7. Interconnected Systems	
8.700. Interconnected Systems Management	8-7-1
ISL 2007-01 #50 (8-700)	

ISL 2007-01 #51 (8-700, 8-701)	
ISL 2007-01 #52 (8-700.d.)	
ISL 2007-01 #53 (8-700.d.)	
8-701. Controlled Interface (CI) Functions.....	8-7-3
ISL 2007-01 #51 (8-700, 8-701)	
8-702. Controller Interface Requirements.....	8-7-3
8-703. Assurances for CIs.....	8-7-4

CHAPTER 9. SPECIAL REQUIREMENTS

Section 1. RD and FRD

ISL 2006-01 #17 (Chapter 9 Section 1)

9-100. General.....	9-1-1
9-101. Authority and Responsibilities.....	9-1-1
9-102. Unauthorized Disclosures.....	9-1-1
9-103. International Requirements.....	9-1-1
9-104. Personnel Security Clearances.....	9-1-1
9-105. Classification.....	9-1-2
9-106. Declassification.....	9-1-2
9-107. Challenges to RD/FRD Classification.....	9-1-2
9-108. Marking.....	9-1-2
9-109. Comingling.....	9-1-3

Section 2. DoD Critical Nuclear Weapon Design Information (CNWDI)

9-200. General.....	9-2-1
9-201. Background.....	9-2-1
9-202. Briefings.....	9-2-1
9-203. Markings.....	9-2-1
9-204. Subcontractors.....	9-2-1
9-205. Transmission Outside the Facility.....	9-2-1
9-206. Records.....	9-2-1
9-207. Weapon Data.....	9-2-1

Section 3. Intelligence Information

ISL 2006-01 #18 (Chapter 9 Section 3)

9-300. Background.....	9-3-1
9-301. Definitions.....	9-3-1
9-302. Key Concepts.....	9-3-1
9-303. Control Markings Authorized for Intelligence Information.....	9-3-2
9-304. Limitation on Dissemination of Classified Intelligence Information.....	9-3-3
9-305. Safeguarding Classified Intelligence Information.....	9-3-3
9-306. Inquiries.....	9-3-3

Section 4. Communication Security (COMSEC)

9-400. General.....	9-4-1
9-401. Instructions.....	9-4-1
9-402. Clearance and Access Requirements.....	9-4-1
9-403. Establishing a COMSEC Account.....	9-4-1
9-404. COMSEC Briefing and Debriefing Requirements.....	9-4-1
9-405. CRYPTO Access Briefing and Debriefing Requirements.....	9-4-2
9-406. Destruction and Disposition of COMSEC Material.....	9-4-2
9-407. Subcontracting COMSEC Work.....	9-4-2
9-408. Unsolicited Proposals.....	9-4-2

CHAPTER 10. INTERNATIONAL SECURITY REQUIREMENTS

Section 1. General and Background Information	
10-100. General	10-1-1
10-101. Applicable Federal Laws	10-1-1
10-102. Bilateral Security Agreements	10-1-1
ISL 2006-02 #21 (10-102)	
Section 2. Disclosure of U.S. Information to Foreign Interests	
10-200. Authorization for Disclosure	10-2-1
10-201. Direct Commercial Arrangements	10-2-1
10-202. Contract Security Provisions	10-2-1
Section 3. Foreign Government Information	
10-300. General	10-3-1
10-301. Contract Security Requirements	10-3-1
10-302. Marking Foreign Government Classified Material	10-3-1
10-303. Foreign Government RESTRICTED Information and “In Confidence” Information	10-3-1
ISL 2006-01 #19 (10-303)	
10-304. Marking U.S. Documents Containing FGI	10-3-1
10-305. Marking Documents Prepared For Foreign Governments	10-3-2
10-306. Storage and Control	10-3-2
ISL 2006-02 #23 (10-306)	
10-307. Disclosure and Use Limitations	10-3-2
ISL 2006-02 #22 (10-307, 10-509 and Appendix C)	
10-308. Transfer	10-3-3
10-309. Reproduction	10-3-3
10-310. Disposition	10-3-3
10-311. Reporting of Improper Receipt of Foreign Government Material	10-3-3
10-312. Subcontracting	10-3-3
Section 4. International Transfers	
10-400. General	10-4-1
10-401. International Transfers of Classified Material	10-4-1
ISL 2006-01 #20 (10-401)	
10-402. Transfers of Freight	10-4-1
ISL 2006-01 #15 (5-412 and 10-402)	
10-403. Return of Material for Repair, Modification, or Maintenance	10-4-2
10-404. Use of Freight Forwarders	10-4-2
10-405. Handcarrying Classified Material	10-4-2
10-406. Classified Material Receipts	10-4-3
10-407. Contractor Preparations for International Transfers Pursuant to Commercial and User Agency Sales	10-4-3
10-408. Transfers Pursuant to an ITAR Exemption	10-4-4
Section 5. International Visits and Control of Foreign Nationals	
10-500. General	10-5-1
10-501. International Visits	10-5-1
10-502. Types and Purpose of International Visits	10-5-1
10-503. Emergency Visits	10-5-1
10-504. Requests for Recurring Visits	10-5-1
10-505. Amendments	10-5-1
10-506. Visits Abroad by U.S. Contractors	10-5-1
10-507. Visits by Foreign Nationals to U.S. Contractor Facilities	10-5-2

10-508. Control of Access by On-Site Foreign Nationals	10-5-3
ISL 2006-02 #24 (10-508.c.)	
ISL 2006-02 #25 (10-508.d.)	
10-509. TCP	10-5-3
ISL 2006-02 #22 (10-307, 10-509 and Appendix C)	
10-510. Security and Export Control Violations Involving Foreign Nationals	10-5-4
Section 6. Contractor Operations Abroad	
10-600. General	10-6-1
10-601. Access by Contractor Employees Assigned Outside the United States	10-6-1
10-602. Storage, Custody, and Control of Classified Information Abroad by Employees of a U.S. Contractor	10-6-1
10-603. Transmission of Classified Material to Employees Abroad	10-6-1
10-604. Security Briefings	10-6-2
Section 7. NATO Information Security Requirements	
10-700. General	10-7-1
10-701. Classification Levels	10-7-1
10-702. NATO RESTRICTED	10-7-1
ISL 2006-01 #21 (10-702)	
10-703. NATO Contracts	10-7-1
10-704. NATO Facility Security Clearance Certificate	10-7-1
10-705. PCL Requirements	10-7-1
10-706. NATO Briefings	10-7-1
10-707. Access to NATO Classified Information by Foreign Nationals	10-7-1
10-708. Subcontracting for NATO Contracts	10-7-2
10-709. Preparing and Marking NATO Documents	10-7-2
10-710. Classification Guidance	10-7-2
10-711. Further Distribution	10-7-2
10-712. Storage of NATO Documents	10-7-2
10-713. International Transmission	10-7-3
10-714. Handcarrying	10-7-3
10-715. Reproduction	10-7-3
10-716. Disposition	10-7-3
10-717. Accountability Records	10-7-3
10-718. Security Violations and Loss, Compromise, or Possible Compromise	10-7-4
10-719. Extracting from NATO Documents	10-7-4
10-720. Release of U.S. Information to NATO	10-7-4
10-721. Visits	10-7-4
Section 8. Transfers of Defense Articles to the United Kingdom without a License or Other Written Authorization	
10-800. General	10-8-1
10-801. Defense Articles	10-8-1
10-802. Marking Requirements	10-8-1
10-803. Transfers	10-8-1
10-804. Records	10-8-1
ISL 2013-03 Transfers of Defense Articles to Australia without a License or Other Written Authorization	

CHAPTER 11. MISCELLANEOUS INFORMATION

Section 1. TEMPEST	
11-100. General	11-1-1
11-101. TEMPEST Requirements	11-1-1
11-102. Cost	11-1-1
Section 2. Defense Technical Information Center (DTIC)	
11-200. General	11-2-1
11-201. User Community	11-2-1
11-202. Registration Process	11-2-1
11-203. Safeguarding Requirements	11-2-1
11-204. DTIC Downgrading or Declassification Notices	11-2-1
11-205. Questions Concerning Reference Material	11-2-1
11-206. Subcontracts	11-2-1
Section 3. Independent Research and Development (IR&D) Efforts	
11-300. General	11-3-1
11-301. Information Generated Under an IR&D Effort that Incorporates Classified Information	11-3-1
11-302. Classification Guidance	11-3-1
11-303. Preparation of Security Guidance	11-3-1
11-304. Retention of Classified Documents Generated Under IR&D Efforts	11-3-1

APPENDIXES

Appendix A. Cognizant Security Office Information	A-1
Appendix B. International Visits Standard Request for Visit Format (RFV)	B-1
Appendix C. Definitions	C-1
Appendix D. ISL Appendixes	D-1

SUPPLEMENTS TO THE NISPOM

NISPOM Supplement	DoD 5220.22-M Sup 1
-------------------	---------------------

REFERENCES

- (a) Executive Order 12829, "National Industrial Security Program," January 6, 1993
- (b) Executive Order 13526, "Classified National Security Information," December 29, 2009
- (c) Section 2011 et seq. of title 42, United States Code, "Atomic Energy Act of 1954," as amended
- (d) Section 403 of title 50, United States Code, "National Security Act of 1947," as amended
- (e) Executive Order 12333, "United States Intelligence Activities," December 8, 1981
- (f) Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004," 118 Stat. 3638, December 17, 2004¹
- (g) Section 781 of title 50, United States Code, "Internal Security Act of 1950"
- (h) Section 552(f) of title 5, United States Code, "Government Organization and Employees"
- (i) DoD 5220.22-C, "Carrier Supplement to the Industrial Security Manual for Safeguarding Classified Information," October 1986
- (j) Title 18 USC, Appendix 3, "Classified Information Procedures Act (CIPA)"
- (k) Section 552 of title 5, United States Code, "Freedom of Information Act"
- (l) Section 552a of title 5, United States Code, "Privacy Act of 1975"
- (m) Section 2170 of Title 50, United States Code Appendix, "Defense Production Act of 1950"
- (n) Intelligence Community Directive 705, "Sensitive Compartmented Information Facilities (SCIFs)," May 26, 2010.
- (o) Underwriters Laboratories, Inc., UL Standard 2050, "National Industrial Security Systems"
- (p) Title 10, Code of Federal Regulations, Part 1045, Subparts A, B, and C, "National Security Information," December 22, 1997
- (q) DoD Instruction 5210.02, "Access to and Dissemination of Restricted Data and Formerly Restricted Data," June 3, 2011
- (r) Department of Energy Order 452.8, "Control of Nuclear Weapon Data," July 21, 2011
- (s) Sections 793, 794, and 798 of title 18, United States Code, Chapter 37, "Espionage and Censorship"
- (t) Section 2751 et seq. of title 22, United States Code, "Arms Export Control Act (AECA)," June 30, 1976, as amended
- (u) App. 2401 et seq. of title 50, United States Code, "The Export Administration Act of 1979 (EAA)," September 29, 1979, as amended
- (v) Title 22, Code of Federal Regulations, Parts 120-130, "International Traffic in Arms Regulations," current edition
- (w) Section 130(c) of title 10, United States Code, "Authority to Withhold from Public Disclosure Certain Technical Data"
- (x) Section 1101(a)(22) and Section 1401, subsection (a) of title 8, United States Code, "Aliens and Nationality"
- (y) Title 15, Code of Federal Regulations, parts 368.1-399.2, "Export Administration Regulation (EAR)," current edition
- (z) Part 2001 of Title 32, Code of Federal Regulations, current edition
- (aa) Information Security Oversight Office Notice 2011-02, "Further Guidance and Clarification on Commingling Atomic Energy Information and Classification National Security Information," May 18, 2011

¹ Not codified

INDUSTRIAL SECURITY LETTERS (ISL) REFERENCES

ISL 2006-01, April 14, 2006
ISL 2006-02, August 22, 2006
ISL 2007-01, October 11, 2007
ISL 2009-01, March 5, 2009
ISL 2009-02, June 6, 2009
ISL 2009-03, November 17, 2009
ISL 2010-01, January 28, 2010
~~ISL 2010-02, February 22, 2010~~ (rescinded by ISL 2013-05)
~~ISL 2011-01, January 13, 2011~~ (rescinded by ISL 2012-04 #2)
ISL 2011-02, April 12, 2011
ISL 2011-03, May 9, 2011
ISL 2011-04, September 23, 2011
ISL 2012-01, February 21, 2012
~~ISL 2012-02, March 11, 2012~~ (rescinded by Change 1 Chapter 10 Section 8)
ISL 2012-03, May 14, 2012
ISL 2012-04, August 7, 2012
ISL 2013-01, January 17, 2013
ISL 2013-02, March 8, 2013
ISL 2013-03, March 20, 2013
ISL 2013-04, June 10, 2013
ISL 2013-05, July 2, 2013
ISL 2013-06, ~~October 4, 2013~~ revised, December 3, 2013
ISL 2014-01, April 14, 2014
ISL 2014-02, April 22, 2014
ISL 2014-03, April 22, 2014

AL1. Acronyms

AL.1.1. AECA	Arms Export Control Act
AL.1.2. ASC	Alarm Service Company
AL.1.3. BL	Bill of Lading
AL.1.4. CAGE	Commercial and Government Entity
AL.1.5. CFIUS	Committee on Foreign Investment in the United States
AL.1.6. CFR	Code of Federal Regulations
AL.1.7. CI	Counterintelligence
AL.1.8. CIA	Central Intelligence Agency
AL.1.9. CM	Configuration Management
AL.1.10. CNWDI	Critical Nuclear Weapons Design Information
AL.1.11. COMSEC	Communications Security
AL.1.12. COR	Central Office of Record
AL.1.13. CRYPTO	Cryptographic
AL.1.14. CSA	Cognizant Security Agency
AL.1.15. CSO	Cognizant Security Office
AL.1.16. CUSR	Central United States Registry
AL.1.17. CVA	Central Verification Activity
AL.1.18. DAA	Designated Accrediting/Approving Authority
AL.1.19. DCID	Director of Central Intelligence Directive
AL.1.20. DGR	Designated Government Representative
AL.1.21. DNI	Director of National Intelligence
AL.1.22. DOD	Department of Defense
AL.1.23. DOE	Department of Energy
AL.1.24. DOJ	Department of Justice
AL.1.25. DSS	Defense Security Service
AL.1.26. DTIC	Defense Technical Information Center
AL.1.27. EAA	Export Administration Act
AL.1.28. EPA	Environmental Protection Agency
AL.1.29. FBI	Federal Bureau of Investigation
AL.1.30. FCC	Federal Communications Commission
AL.1.31. FCL	Facility (Security) Clearance
AL.1.32. FGI	Foreign Government Information
AL.1.33. FOCI	Foreign Ownership, Control or Influence
AL.1.34. FOUO	For Official Use Only
AL.1.35. FRD	Formerly Restricted Data
AL.1.36. FRS	Federal Reserve System
AL.1.37. FSCC	NATO Facility Security Clearance Certificate
AL.1.38. FSO	Facility Security Officer
AL.1.39. GAO	Government Accountability Office
AL.1.41. GCMS	Government Contractor Monitoring Station
AL.1.42. GFE	Government Furnished Equipment
AL.1.43. GSA	General Services Administration
AL.1.44. GSC	Government Security Committee

AL.1.45. IC	Intelligence Community
AL.1.46. IDS	Intrusion Detection System
AL.1.47. IFB	Invitation for Bid
AL.1.48. IR&D	Independent Research & Development
AL.1.49. IS	Information System
AL.1.50. ISCAP	Interagency Security Classification Appeals Panel
AL.1.51. ISOO	Information Security Oversight Office
AL.1.52. ISSM	Information System Security Manager
AL.1.53. ISSO	Information System Security Officer
AL.1.54. ITAR	International Traffic in Arms Regulations
AL.1.55. LAA	Limited Access Authorization
AL.1.56. LAN	Local Area Network
AL.1.57. MFO	Multiple Facility Organization
AL.1.58. NACLC	National Agency Check with Local Agency Check and Credit Check
AL.1.59. NASA	National Aeronautics and Space Administration
AL.1.60. NATO	North Atlantic Treaty Organization
AL.1.61. NIAG	NATO Industrial Advisory Group
AL.1.62. NID	National Interest Determination
AL.1.63. NISP	National Industrial Security Program
AL.1.64. NISPOM	National Industrial Security Program Operating Manual
AL.1.65. NISPOMSUP	National Industrial Security Program Operating Manual Supplement
AL.1.66. NOFORN	Not Releasable to Foreign Nationals
AL.1.67. NPLO	NATO Production Logistics Organization
AL.1.68. NRC	Nuclear Regulatory Commission
AL.1.69. NSA	National Security Agency
AL.1.70. NSF	National Science Foundation
AL.1.71. NSI	National Security Information
AL.1.72. OADR	Originating Agency's Determination Required
AL.1.73. ORCON	Dissemination and Extraction of Information Controlled by Originator
AL.1.74. PCL	Personnel (Security) Clearance
AL.1.75. PROPIN	Proprietary Information Involved
AL.1.77. RDT&E	Research, Development, Technical and Engineering
AL.1.78. REL TO	Authorized for Release to
AL.1.79. RFP	Request for Proposal
AL.1.80. RFQ	Request for Quotation
AL.1.81. RFV	Request for Visit
AL.1.82. SAP	Special Access Program
AL.1.83. SBA	Small Business Administration
AL.1.84. SCA	Security Control Agreement
AL.1.85. SCI	Sensitive Compartmented Information
AL.1.86. SCIF	Sensitive Compartmented Information Facility
AL.1.87. SDDC	Surface Deployment and Distribution Command
AL.1.88. SIO	Senior Intelligence Officer

AL.1.89. SOIC	Senior Official of the Intelligence Community
AL.1.90. SSA	Special Security Agreement
AL.1.91. SSBI	Single Scope Background Investigation
AL.1.92. SSP	Systems Security Plan
AL.1.93. TCO	Technology Control Officer
AL.1.94. TCP	Technology Control Plan
AL.1.95. TP	Transportation Plan
AL.1.96. UL	Underwriters' Laboratories
AL.1.97. USAID	United States Agency for International Development
AL.1.98. USC	United States Code
AL.1.99. USCIS	United States Citizenship and Immigration Services
AL.1.100. USITC	United States International Trade Commission
AL.1.101. USML	United States Munitions List
AL.1.102. USTR	United States Trade Representative
AL.103. VAL	Visit Authorization Letter

CHAPTER 1

General Provisions and Requirements

Section 1. Introduction

1-100. Purpose. This Manual is issued in accordance with the National Industrial Security Program (NISP). It prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including Restricted Data (RD), Formerly Restricted Data (FRD), intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations.

1-101. Authority

a. The NISP was established by Executive Order (E.O.) 12829 (reference (a)) for the protection of information classified under E.O. 13526 (reference (b)), or its successor or predecessor orders, and the Atomic Energy Act of 1954, as amended (reference (c)). The National Security Council is responsible for providing overall policy direction for the NISP. The Secretary of Defense has been designated Executive Agent for the NISP by the President. The Director, Information Security Oversight Office (ISOO), is responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies.

b. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission (NRC) and the Director of National Intelligence (DNI) is responsible for the issuance and maintenance of this Manual.

(1) The Secretary of Energy and the Chairman of the NRC are responsible for prescribing

that portion of the Manual that pertains to information classified under reference (c). Additionally, the Secretary of Energy and the Chairman of the NRC retain authority over access to information under their respective programs classified under reference (c), and may inspect and monitor contractor, licensee, certificate holder, and grantee programs and facilities that involve access to such information.

(2) The DNI is responsible for prescribing that portion of the Manual that pertains to intelligence sources and methods, including SCI. The DNI retains authority over access to intelligence sources and methods, including SCI. The DNI's responsibilities are derived from the National Security Act of 1947, as amended (reference (d)); Executive Order (EO) 12333, as amended (reference (e)); reference (b); and The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (reference (f)). For purposes of this Manual, the DNI may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information.

c. The Secretary of Defense serves as Executive Agent for inspecting and monitoring contractors, licensees, grantees, and certificate holders who require or will require access to, or who store or will store classified information; and for determining the eligibility for access to classified information of contractors, licensees, certificate holders, and grantees and their respective employees.

d. The Director, ISOO, will consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the NISP.

e. Nothing in this Manual shall be construed to supersede the authority of the Secretary of Energy or the Chairman of the NRC under reference (c). Nor shall this information detract from the authority of installation commanders under the Internal Security Act of 1950 (reference (g)); or the authority of the DNI under reference (f). This Manual shall not

detract from the authority of other applicable provisions of law, or the authority of any other Federal department or agency head granted according to U.S. statute or Presidential decree.

1-102. Scope

ISL 2006-01 #1 (1-102). All changes reflected in the February 28, 2006 issuance of the NISPOM must be implemented no later than 6 months from the publication date; that is, by September 1, 2006.

When a change to the NISPOM eliminates a requirement, the contractor may elect to continue that particular practice or procedure for operational necessity or convenience. However, such practices or procedures will not be subject to DSS inspection or oversight. In addition, DSS will not cite contractors for imposing processes or procedures that are no longer required, unless they are expressly prohibited in the NISPOM.

a. The NISP applies to all Executive Branch Departments and Agencies and to all cleared contractor facilities located within the United States and its territories.

b. This Manual applies to and shall be used by contractors to safeguard classified information released during all phases of the contracting, licensing, and grant process, including bidding, negotiation, award, performance, and termination. It also applies to classified information not released under a contract, license, certificate or grant, and to foreign government information furnished to contractors that requires protection in the interest of national security. This Manual implements applicable Federal statutes, E.O.s, national directives, international treaties, and certain government-to-government agreements.

c. Implementation of changes to this Manual by contractors shall be effected no later than 6 months from the date of the published change, with the exception of changes related to US-UK Treaty requirements, in Chapter 10, Section 8 of this Manual, which must be implemented immediately.

d. This Manual does not contain protection requirements for Special Nuclear Material.

1-103. Agency Agreements

a. Reference (a) requires the Heads of Agencies to enter into agreements with the Secretary of Defense as the Executive Agent for the NISP. This is designated by Presidential guidance that establishes the terms of the Secretary's responsibilities on behalf of these agency heads.

b. The Secretary of Defense has entered into agreements with the departments and agencies listed below for the purpose of rendering industrial security services. This delegation of authority is contained in an exchange of letters between the Secretary of Defense and (1) the Administrator, National Aeronautics and Space Administration (NASA); (2) the Secretary of Commerce; (3) the Administrator, General Services Administration (GSA); (4) the Secretary of State; (5) the Administrator, Small Business Administration (SBA); (6) the Director, National Science Foundation (NSF); (7) the Secretary of the Treasury; (8) the Secretary of Transportation; (9) the Secretary of the Interior; (10) the Secretary of Agriculture; (11) the Secretary of Labor; (12) the Administrator, Environmental Protection Agency (EPA); (13) the Attorney General, Department of Justice (DOJ); (14) the Chairman, Board of Governors, Federal Reserve System (FRS); (15) the Comptroller General of the United States, Government Accountability Office (GAO); (16) the Director of Administrative Services, United States Trade Representative (USTR); (17) the Director of Administration, United States International Trade Commission (USITC); (18) the Administrator, United States Agency for International Development (USAID); (19) the Executive Director for Operations of the NRC; (20) the Secretary of Education; (21) the Secretary of Health and Human Services; (22) the Secretary of Homeland Security; (23) the Deputy Managing Director, Federal Communications Commission (FCC); and (24) the Deputy Director, Facilities, Security, and Contracting, Office of Personnel Management.

ISL 2012-01 (1-103.b.). Executive Order 12829 (January 6, 1993, as amended), "National Industrial Security Program" (NISP), states that the heads of Federal agencies shall enter into agreements with the Secretary of Defense that establish the terms of the Secretary's NISP responsibilities on behalf of those agency heads.

DoD 5220.22-M, "National Industrial Security Program Operating Manual" (NISPOM), February 28, 2006, paragraph 1-103.b. lists the 23 non-Department of Defense (DoD) agencies that entered into agreements for industrial security services with the Secretary of Defense as of the date the NISPOM was published. That list is now amended, as the Department of Defense and the Office of Personnel Management (OPM) entered into an agreement on February 21, 2012 that makes OPM the 24th non-DoD agency for which DoD will provide industrial security services.

ISL 2013-02 (1-103.b.). Executive Order 12829 (January 6, 1993, as amended), "National Industrial Security Program" (NISP), states that the heads of Federal agencies shall enter into agreements with the Secretary of Defense that establish the terms of the Secretary's NISP responsibilities on behalf of those agency heads. NISPOM paragraph 1-103.b. lists the non-Department of Defense (DoD) agencies that have agreements for industrial security services with DoD.

The list is now amended to include the National Archives and Records Administration (NARA), which entered into an agreement with the Department of Defense on March 8, 2013. This addition makes NARA the 25th non-DoD agency for which DoD will provide industrial security services.

ISL 2013-04 (1-103.b.). The list is now amended to include the Overseas Private Investment Corporation (OPIC), which entered into an agreement with the Department of Defense on June 10, 2013. This addition makes OPIC the 26th non-DoD agency for which DoD will provide industrial security services.

ISL 2014-02 (1-103.b.). The list is now amended to include the U.S. Department of Housing and Urban Development (HUD), which entered into an agreement with the Department of Defense on April 22, 2014. This addition makes HUD the 27th non-DoD agency for which DoD will provide industrial security services.

1-104. Security Cognizance

a. Consistent with paragraph 1-101e, security cognizance remains with each Federal department or agency unless lawfully delegated. The term

Cognizant Security Agency (CSA) denotes the Department of Defense (DoD), the Department of Energy (DOE), the NRC, and the DNI. The Secretary of Defense, the Secretary of Energy, the DNI and the Chairman, NRC, may delegate any aspect of security administration regarding classified activities and contracts under their purview within the CSA or to another CSA. Responsibility for security administration may be further delegated by a CSA to one or more Cognizant Security Offices (CSO). It is the obligation of each CSA to inform industry of the applicable CSO.

b. The designation of a CSO does not relieve any Government Contracting Activity (GCA) of the responsibility to protect and safeguard the classified information necessary for its classified contracts, or from visiting the contractor to review the security aspects of such contracts.

c. Nothing in this Manual affects the authority of the Head of an Agency to limit, deny, or revoke access to classified information under its statutory, regulatory, or contract jurisdiction if that Agency Head determines that the security of the nation so requires. The term "Agency Head" has the meaning provided in Title 5 United States Code (U.S.C.) Section 552(f) (reference (h)).

1-105. Composition of Manual. This Manual is comprised of a "baseline" portion (Chapters 1 through 11). The portion of the Manual that prescribes requirements, restrictions, and safeguards that exceed the baseline standards, such as those necessary to protect special classes of information, is included in the NISPOM Supplement (NISPOMSUP). Until officially revised or canceled, the existing Carrier Supplement to the former "Industrial Security Manual for Safeguarding Classified Information" (reference (i)) will continue to be applicable to DoD-cleared facilities only.

1-106. Manual Interpretations. All contractor requests for interpretations of this Manual shall be forwarded to the CSA through its designated CSO. Requests for interpretation by contractors located on any U.S. Government installation shall be forwarded to the CSA through the commander or head of the host installation. Requests for interpretation of Director of Central Intelligence Directives (DCIDs)

shall be forwarded to the DNI through approved channels.

1-107. Waivers and Exceptions to this Manual.

Requests shall be submitted by industry through government channels approved by the CSA. When submitting a request for waiver, the contractor shall specify, in writing, the reasons why it is impractical or unreasonable to comply with the requirement. Waivers and exceptions will not be granted to impose more stringent protection requirements than this Manual provides for CONFIDENTIAL, SECRET, or TOP SECRET information.

Section 2. General Requirements

1-200. General. Contractors shall protect all classified information to which they have access or custody. A contractor performing work within the confines of a Federal installation shall safeguard classified information according to the procedures of the host installation or agency.

ISL 2006-02 #1 (1-200). Security for Wireless Devices, Services and Technologies (ISL 05L-1 #10). NISPOM paragraph 1-200 states that "Contractors shall protect all classified information to which they have access or custody." Therefore, industry should implement security procedures to mitigate risks associated with wireless devices in areas where employees are working with classified information and/or where classified discussions may be held. Facility Security Officers must consider the capabilities of the wireless device and use sound judgment in developing appropriate security countermeasures. Depending on the device/technology, appropriate security countermeasures may range from ensuring a wireless device is turned off or not used in classified areas to, in some cases, not permitting the devices in the area.

1-201. Facility Security Officer (FSO). The contractor shall appoint a U.S. citizen employee, who is cleared as part of the facility clearance (FCL) to be the FSO. The FSO will supervise and direct security measures necessary for implementing applicable requirements of this Manual and related Federal requirements for classified information. The FSO, or those otherwise performing security duties, shall complete security training as specified in Chapter 3 and as deemed appropriate by the CSA.

1-202. Standard Practice Procedures. The contractor shall implement all applicable terms of this Manual at each of its cleared facilities. Written procedures shall be prepared when the FSO believes them to be necessary for effective implementation of this Manual or when the CSA determines them to be necessary to reasonably exclude the possibility of loss or compromise of classified information.

1-203. One-Person Facilities. A facility at which only one person is assigned shall establish procedures for CSA notification after death or incapacitation of that person. The current combination of the facility's

security container shall be provided to the CSA, or in the case of a multiple facility organization, to the home office.

1-204. Cooperation with Federal Agencies and Officially Credentialed Representatives of Those Agencies. Contractors shall cooperate with Federal agencies and their officially credentialed representatives during official inspections, investigations concerning the protection of classified information, and during personnel security investigations of present or former employees and others. Cooperation includes providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours, providing relevant employment and security records for review when requested, and rendering other necessary assistance.

ISL 2006-01 #2 (1-204). Contractor investigators and any other contractor personnel who may carry official credentials issued by the Department of Defense, the Office of Personnel Management (OPM), or any other Federal Agency are to be afforded the same level of cooperation as required for officially credentialed government representatives. Those most likely to be encountered are contractor investigators credentialed by OPM conducting personnel security (i.e. background) investigations.

ISL 2010-01 #1 (1-204). This article provides clarification of the requirement in NISPOM paragraph 1-204 for contractors to cooperate with Federal agencies and their officially credentialed representatives during personnel security (i.e., "background") investigations of present or former employees and others. The term "cooperation" in this NISPOM paragraph means providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours, providing relevant employment and security records for review when requested, and rendering other necessary assistance.

Relevant employment records include all personnel files, security records, supervisory files, and other records pertaining to the individual under investigation, and in the possession, or under the control of the contractor's representatives or offices.

Simply referring an investigator to an automated (telephone or computer) employment verification service is not sufficient for a personnel security investigation. It is necessary that employment files be reviewed during the course of a personnel security investigation for purposes beyond merely verifying the date(s) of employment and eligibility for rehire. On-scene investigators must be able to compare information in the employment record with the information listed by the applicant on the personnel security questionnaire to determine if there are discrepancies or variances.

Investigators also need to ascertain if the records contain any information that pertains to or may be relevant to the adjudication of the person's eligibility for access to classified information, such as garnishments, excessive absenteeism, security violations, etc.

Contractor investigators and any other contractor personnel who carry official credentials issued by the Department of Defense, the Office of Personnel Management (OPM), or any other Federal Agency who are conducting personnel security investigations are to be afforded the same level of cooperation as required for officially credentialed government representatives. Those most likely to be encountered are contractor investigators credentialed by OPM conducting personnel security investigations.

1-205. Security Training and Briefings. Contractors are responsible for advising all cleared employees, including those outside the United States, of their individual responsibility for safeguarding classified information. In this regard, contractors shall provide security training as appropriate, according to Chapter 3, to cleared employees by initial briefings, refresher briefings, and debriefings.

1-206. Security Reviews

ISL 2006-02 #2 (1-206). Security Review Ratings (ISL 04L-1 #8). DSS assigns a security rating to contractor facilities at the conclusion of each security review. The security rating is the Industrial Security Representative's overall assessment of the effectiveness of the security systems and procedures in place to protect classified information at the facility. Following is a brief summary of the criteria for each rating category.

- **Superior:** A Superior rating is reserved for contractors who have consistently and fully implemented the requirements of the NISPOM in an effective fashion resulting in a superior security posture, compared with other contractors of similar size and complexity. The facility must have documented procedures that heighten the security awareness of the contractor employees and that foster a spirit of cooperation within the security community. This rating requires a sustained high level of management support for the security program and the absence of any serious security issues. For more complex facilities, minimal administrative findings are allowable.
- **Commendable:** A Commendable rating is assigned to contractors who have fully implemented the requirements of the NISPOM in an effective fashion resulting in a commendable security posture, compared with other contractors of similar size and complexity. This rating denotes a security program with strong management support, the absence of any serious security issues and minimal administrative findings.
- **Satisfactory:** Satisfactory is the most common rating and denotes that a facility's security program is in general conformity with the basic requirements of the NISPOM. This rating may be assigned even though there were findings in one or more of the security program elements. Depending on the circumstances, a Satisfactory rating can be assigned even if there were isolated serious findings during the security review.
- **Marginal:** A Marginal rating indicates a substandard security program. This rating signifies a serious finding in one or more security program areas that could contribute to the eventual compromise of classified information if left uncorrected. The facility's size, extent of classified activity, and inherent nature of the problem are considered before assigning this rating. A compliance security review is required within a specified period to assess the actions taken to correct the findings that led to the Marginal rating.

- **Unsatisfactory:** Unsatisfactory is the most serious security rating. An Unsatisfactory rating is assigned when circumstances and conditions indicate that the facility has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified material in its possession or to which it has access. This rating is appropriate when the security review indicates that the contractor's security program can no longer preclude the disclosure of classified information to unauthorized persons. When an Unsatisfactory rating is assigned, the applicable government contracting activities are notified of the rating and the circumstances on which that rating was based. In addition, a compliance security review must be conducted after a specified interval to assess the corrective actions taken before the contractor's security rating can return to the Satisfactory level.

a. **Government Reviews.** Aperiodic security reviews of all cleared contractor facilities will be conducted to ensure that safeguards employed by contractors are adequate for the protection of classified information.

(1) **Review Cycle.** The CSA will determine the frequency of security reviews, which may be increased or decreased consistent with risk management principles. Security reviews may be conducted not more often than once every 12 months unless special circumstances exist.

(2) **Procedures.** Contractors will normally be provided notice of a forthcoming review. Unannounced reviews may be conducted at the discretion of the CSA. Security reviews necessarily subject all contractor employees and all areas and receptacles under the control of the contractor to examination. However, every effort will be made to avoid unnecessary intrusion into the personal effects of contractor personnel. The physical examination of the interior space of equipment not authorized to secure classified material will always be accomplished in the presence of a representative of the contractor.

(3) **Reciprocity.** Each CSA is responsible for ensuring that redundant and duplicative security review and audit activity of its contractors is held to a minimum, including such activity conducted at

common facilities by other CSA's. Appropriate intra-and/or inter-agency agreements shall be executed to avoid redundant and duplicate reviews. Instances of redundant and duplicative security review and audit activity shall be reported to the Director, ISOO, for resolution.

b. **Contractor Reviews.** Contractors shall review their security system on a continuing basis and shall also conduct a formal self-inspection at intervals consistent with risk management principles.

1-207. Hotlines. Federal agencies maintain hotlines to provide an unconstrained avenue for government and contractor employees to report, without fear of reprisal, known or suspected instances of serious security irregularities and infractions concerning contracts, programs, or projects. These hotlines do not supplant contractor responsibility to facilitate reporting and timely investigation of security matters concerning its operations or personnel, and contractor personnel are encouraged to furnish information through established company channels. However, the hotline may be used as an alternate means to report this type of information when considered prudent or necessary. Contractors shall inform all employees that the hotlines may be used, if necessary, for reporting matters of national security significance. CSA hotline addresses and telephone numbers are as follows:

Defense Hotline
The Pentagon
Washington, DC 20301-1900
(800) 424-9098

U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program, MS 05 E13
11555 Rockville Pike
Rockville, MD 20852-2738
1-800-233-3497
TDD: 1-800-270-2787

CIA Hotline
Office of the Inspector General
Central Intelligence Agency
Washington, D.C. 20505
(703) 874-2600

DOE Hotline
Department of Energy
Office of the Inspector General
1000 Independence Avenue, S.W. Room SD-031
Washington, D.C. 20585
(202) 586-4073
(800) 541-1625

DNI Hotline
Director of National Intelligence
Office of the Inspector General
Washington, D.C. 20511
(703) 482-2650

1-208. Classified Information Procedures Act (CIPA) (Public Law. 96-456, 94 Stat. 2025 codified at Title 18 U.S.C. Appendix 3 (reference (j))). The CIPA provides procedures for access to classified information by defendants and their representatives in criminal proceedings in U.S. District Courts, U.S. Courts of Appeal, and the U.S. Supreme Court. The provisions of this Manual do not apply to criminal proceedings in the courts and do not authorize contractors or their employees to release classified information in connection with any criminal proceedings.

Section 3. Reporting Requirements

1-300. General. Contractors are required to report certain events that have an impact on the status of the facility clearance (FCL), that impact on the status of an employee's personnel security clearance (PCL), that affect proper safeguarding of classified information, or that indicate classified information has been lost or compromised. Contractors shall establish such internal procedures as are necessary to ensure that cleared employees are aware of their responsibilities for reporting pertinent information to the FSO, the Federal Bureau of Investigation (FBI), or other Federal authorities as required by this Manual, the terms of a classified contract, and U.S. law. Contractors shall provide complete information to enable the CSA to ascertain whether classified information is adequately protected. Contractors shall submit reports to the FBI and to their CSA as specified in this section.

a. When the reports are classified or offered in confidence and so marked by the contractor, the information will be reviewed by the CSA to determine whether it may be withheld from public disclosure under applicable exemptions of the Freedom of Information Act (5 U.S.C. 552) (reference (k)).

b. When the reports are unclassified and contain information pertaining to an individual, the Privacy Act of 1974 (5 U.S.C. 552a)(reference (l)) permits withholding of that information from the individual only to the extent that the disclosure of the information would reveal the identity of a source who furnished the information to the U.S. Government under an expressed promise that the identity of the source would be held in confidence. The fact that a report is submitted in confidence must be clearly marked on the report.

1-301 Reports to be Submitted to the FBI. The contractor shall promptly submit a written report to the nearest field office of the FBI regarding information coming to the contractor's attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations. An initial report may be made by phone, but it must be followed in writing, regardless of the disposition made of the report by the FBI. A

copy of the written report shall be provided to the CSA.

ISL 2013-05 (1-301). Reporting Requirements to Cyber Intrusions. ISL 2010-02 is hereby cancelled and superseded by this ISL, which clarifies the application of NISPOM paragraph 1-301 reporting requirements to cyber intrusions occurring on contractor information systems.

The NISPOM is focused on the protection of classified information, and specifically covers classified information systems owned or operated by cleared industry. The NISPOM does not govern the protection of unclassified information, nor does it provide security or reporting requirements that are directed to a contractor's unclassified information systems.

It is in this context that paragraph 1-301 of the NISPOM requires contractors¹ to promptly report to the Federal Bureau of Investigation (FBI) (with a copy to DSS) information coming to the contractor's attention concerning "actual, probable or possible espionage, sabotage, terrorism, or subversive activities" at any of the contractor's locations. The purpose of this requirement is to identify specific types of threat activity at contractor facilities that pose a risk to the protection of classified information, systems, or programs. Although this requirement is not directed to unclassified information or systems, contractors must report activities that otherwise meet the threshold for reporting, including activities that may have occurred on its unclassified information systems.

More specifically, a cyber-intrusion² may fall under the reporting requirements of NISPOM paragraph 1-301, regardless of the classification level of information or information system involved in the intrusion, provided that the contractor has determined that (i) the facts and circumstances of the intrusion are sufficient to qualify as "actual, probable, or possible espionage, sabotage, terrorism, or subversive activities," and (ii) these activities constitute a threat to the protection of classified information, information systems, or programs that are otherwise covered by the NISPOM.

Thus, paragraph 1-301 does not establish a broad based reporting requirement regarding cyber incidents or intrusions occurring on the contractor's unclassified information systems – it is only directed to those intrusions that by their very nature are so serious as to pose a threat to classified information, systems, or programs.

When analyzing whether a cyber-intrusion appears to meet the reporting threshold, it may be beneficial to consider established criteria for such significant threat activities. For example, Title 18, United States Code, characterizes espionage as “obtaining information about the national defense with intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation,” and economic espionage as including “knowingly performing targeting or acquisition of trade secrets to knowingly benefit any foreign government, foreign instrumentality, or foreign agent.”³

Although the NISPOM does not cover the protection of unclassified information or information systems, there are several other initiatives in these areas. For example, the Defense Industrial Base Cyber Security and Information Assurance (DIB CS/IA) program.⁴ In addition, the Department of Defense is developing implementation guidance for National Defense Authorization Act for Fiscal Year 2013 Section 941, “Reports to Department of Defense on Penetrations of Networks and Information Systems of Certain Contractors,” which will clarify reporting of cyber incidents on contractor information systems, and should help resolve any confusion or potential overlap of activities under the DIB CS/IA program, the proposed DFARS revisions, and the NISPOM.

¹ As defined by the NISPOM, a “contractor” is any “industrial, educational, commercial or other entity that has been granted a facility clearance.”

² An intrusion, as defined in the National Information Assurance Glossary, Committee on National Security Systems Instruction No. 4009, is the “unauthorized act of bypassing the security mechanisms of a system.”

³ Sections 793 and 1831, respectively, of Title 18, U.S.C.

⁴ See Part 236, “Department of Defense [DIB] Voluntary [CS/IA] Activities,” of Title 32, Code of Federal

Regulations, established by interim final rule published on May 11, 2012 (77 FR 27615).

1-302 Reports to be Submitted to the CSA

ISL 2006-02 #3 (1-302). Reporting Participation in Rehabilitation Programs as Adverse Information (ISL 00L-1 #3). There is some confusion regarding the requirement to report participation in rehabilitation program as adverse information, particularly when the company promises “confidentiality” to employees who enroll. Therefore, the following guidance is provided:

- Self-enrollment in a rehabilitation program is not necessarily reportable. However, alcohol and drug abuse, or observation of behavior which is indicative of alcohol or drug abuse is reportable.
- Mandatory enrollment in an Employee Assistance Program is reportable.
- Refusal to accept rehabilitation assistance when offered is reportable.
- Incomplete or unsuccessful participation in a rehabilitation program is reportable.

The above policy interpretation is intended to provide a balance between industry's need for rehabilitation programs which do not necessarily have adverse consequences for enrollment, and the Government's need to properly monitor cleared individuals' continued eligibility for access to classified information. Participation in a rehabilitation program should not be used as a shield to prevent scrutiny by the Government. Keep in mind that the adverse information report is never the sole basis for suspension or revocation of a clearance.

ISL 2006-02 #4 (1-302, 1-303, 1-304). Reports Submitted to the CSA (ISL 02L-1 #9). The following report relating to NISPOM paragraph 1-302 will be made in JPAS:

- Change in Cleared Employee Status

The following reports relating to NISPOM paragraph 1-302 will be submitted to DISCO:

- Adverse Information

- Citizenship by Naturalization
- Employees Desiring Not to Perform on Classified Work
- Refusal by an employee to execute the SF-312

The following reports relating to NISPOM paragraph 1-302 will be submitted to the DSS Field Office:

- Suspicious Contacts
- Changed Conditions Affecting the FCL
- Change in Storage Capability
- Inability to Safeguard Classified Material
- Security Equipment Vulnerabilities
- Unauthorized Receipt of Classified Material
- Employee Information in Compromise Cases
- Disposition of Classified Material Terminated from Accountability
- Foreign Classified Contracts

a. Adverse Information. Contractors shall report adverse information coming to their attention concerning any of their cleared employees. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. If the individual is employed on a Federal installation, the contractor shall furnish a copy of the report and its final disposition to the commander or head of the installation.

NOTE: In *Taglia vs. Philco* (372 F.2d 771), the U.S. Court of Appeals for the 4th Circuit decided that a contractor is not liable for defamation of an employee because of reports made to the Government under the requirements of this Manual and its previous versions. In *Becker v. Philco* (389 U.S. 979), the U.S. Supreme Court denied the appeal from the 4th Circuit.

ISL 2011-04 (1-302.a). “National Industrial Security Program Operating Manual” (NISPOM) requires that contractors report to DSS any adverse information coming to their attention concerning their cleared employees¹. Adverse information consists of any information that negatively reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security. Examples of adverse

information include culpability for security violations meeting the criteria of paragraph 1-304, NISPOM, use of illegal drugs, excessive use of alcohol, wage garnishments or other indications of financial instability, repeated instances of failing to follow established security procedures, the unauthorized release of classified information and/or unauthorized access to classified information systems, or other violations of information systems security requirements.

Contractors are reminded that any adverse information coming to their attention regarding cleared employees must be reported for the full duration of the individual’s employment with the company. An individual’s anticipated departure or termination of employment, for whatever reason, and whether imminent or not, does not change the contractor’s reporting responsibility.

Adverse information reports submitted pursuant to NISPOM 1-302a should be recorded as an incident report in the Joint Personnel Adjudication System (JPAS). The Defense Industrial Security Clearance Office (DISCO) will make a final determination of continued eligibility.

¹ Cleared employees: All contractor employees granted personnel security clearances (PCLs) and all employees being processed for PCLs (Appendix C, “Definitions,” NISPOM).

b. Suspicious Contacts. Contractors shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. In addition, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country shall be reported.

c. Change in Cleared Employee Status. Contractors shall report: (1) the death; (2) a change in name; (3) the termination of employment; (4) change in citizenship; and (5) when the possibility of access to classified information in the future has been reasonably foreclosed. The CSA shall designate the appropriate reporting mechanism.

d. Citizenship by Naturalization. Contractors shall report if a non-U.S. citizen employee granted a Limited Access Authorization (LAA) becomes a citizen through naturalization. The report shall include: (1) city, county, and state where naturalized; (2) date naturalized; (3) court; and (4) certificate number.

e. Employees Desiring Not to Perform on Classified Work. Contractors shall report that an employee no longer wishes to be processed for a clearance or to continue an existing clearance.

f. Standard Form (SF) 312. Refusal by an employee to execute the "Classified Information Nondisclosure Agreement" (SF 312).

g. Change Conditions Affecting the Facility Clearance

(1) Any change of ownership, including stock transfers that affect control of the company.

(2) Any change of operating name or address of the company or any of its cleared locations.

(3) Any change to the information previously submitted for key management personnel including, as appropriate, the names of the individuals they are replacing. In addition, a statement shall be made indicating (a) whether the new key management personnel are cleared, and if so, to what level and when, their dates and places of birth, social security numbers, and their citizenship; (b) whether they have been excluded from access; or (c) whether they have been temporarily excluded from access pending the granting of their clearance. A new complete listing of key management personnel need be submitted only at the discretion of the contractor and/or when requested by the CSA.

(4) Action to terminate business or operations for any reason, imminent adjudication or

reorganization in bankruptcy, or any change that might affect the validity of the FCL.

(5) Any material change concerning the information previously reported by the contractor concerning foreign ownership, control or influence (FOCI). This report shall be made by the submission of a Certificate Pertaining to Foreign Interests. When submitting this information, it is not necessary to repeat answers that have not changed. When entering into discussions, consultations or agreements that may reasonably lead to effective ownership or control by a foreign interest, the contractor shall report the details by letter. If the contractor has received a Schedule 13D from the investor, a copy shall be forwarded with the report.

ISL 2009-03 (1-302.g.(5) and 2-302)

Q: What constitutes a reportable material change under the National Industrial Security Program Operating Manual (NISPOM) paragraph 1-302g (5) or a reportable significant change under NISPOM paragraph 2-302?

A: While nothing in this ISL modifies the current reporting obligations, including but not limited to those under NISPOM paragraph 1-302g (1) through (4) or the rights of DoD to determine significance for purpose of NISPOM paragraph 2-300e, the following matrix describes circumstances that business organizations are required to report on the Standard Form 328, Certificate Pertaining to Foreign Interests, to the Defense Security Service (DSS). When submitting information, it is not necessary to repeat answers that have not changed.

Please note that this matrix is not an exhaustive list of circumstances. It may be revised based on factors such as emerging financial instruments and the experiences of government activities responsible for the oversight of Foreign Ownership, Control or Influence (FOCI) affecting the protection of classified information in industry.

SF 328 Question		Changed Conditions Requiring Report (Note: In addition to the situations described below, <u>all</u> circumstances that would change any answer on the SF 328 from "No" to "Yes" must be reported by submitting a changed condition SF 328.)
1.a.	Where a foreign interest owns five	Five percent (5%) or greater increase in the beneficial ownership of a

	percent (5%) or more of a U.S. business organization	class of equity securities of the business organization, as determined by voting or investment rights, by one or more foreign interests as defined in NISPOM Appendix C and any U.S. person effectively controlled by a foreign interest.
1.b.	Where a foreign interest owns five percent (5%) or more of a U.S. business organization that does not issue stock	Five percent (5%) or greater increase in the beneficial ownership of the business organization, as determined by voting or investment rights, by one or more foreign interests as defined in NISPOM Appendix C and any U.S. person effectively controlled by a foreign interest.
2.	Where a U.S. business organization owns ten percent (10%) or more of a foreign interest	Any increase equivalent to 10% or more of the tangible net worth of the business organization.
3.	Where a U.S. business organization has non-U.S. citizen Key Management Personnel (KMP)	Appointment of any additional non-U.S. citizen to a position required to be cleared in connection with the facility clearance or to any position identified in the articles of incorporation, by-laws, articles of organization, or equivalent governance documentation or charter for the business organization.
4.	Where a Foreign Person has the power to control selection or tenure of KMPs/other decisions	Any change in such power/authority except amendments or waivers to governance documentation either to correct manifest error or which are of a formal, minor, or technical nature and do not change materially any person's rights or obligations.
5.	Where there are contracts, agreements, understandings, arrangement with foreign person(s)	Any change expected to result in annual payments to or from an entity where the payments exceed twenty percent (20%) of the U.S. business organization's annual gross revenues.
6.	Where there is indebtedness, liabilities or obligations to foreign persons	There is a changed condition reportable on SF 328 whenever there is: (i) any new indebtedness to foreign persons which results in a liability exceeding ten percent (10%) of the tangible net worth of the business organization or includes an instrument creating a mortgage, deed of trust, pledge, lien, security interest or other charge or encumbrance against (A) any of its property, assets or leasehold interests exceeding ten percent (10%) of the business organization's tangible net worth or (B) pledges five percent (5%) or more of the voting securities of the business organization as collateral or (ii) any other new foreign indebtedness where the business organization permits to exist a leverage ratio exceeding two to one (2:1) based on the business organization's indebtedness to its tangible net worth and calculated on the basis of information set forth in its financial statements.
7.a.	Where the business organization derives five percent (5%) or more of total revenues/net income from a single foreign person	With respect to the business organization and that single foreign person, any change expected to result in annual payments to or from the business organization where the payments exceed an additional ten percent (10%) of the business organization's annual gross revenues.
7.b.	Where the business organization derives thirty percent (30%) or more of total revenues/net income from foreign persons	With respect to the business organization and any foreign persons, any change expected to result in annual payments to or from the business organization where the payments exceed an additional twenty percent (20%) of the business organization's annual gross revenues.
8.	Where there are ten percent (10%) or more of voting securities held in a method which does not identify beneficial owner	Any change of five percent (5%) or more in the total number of shares held in "nominee" shares, in "street names" or in some other method which does not identify the beneficial owner or any amendment to the bylaws of the business organization or its parent related specifically to

		voting rights of such nominee holders and any requirements regarding notice of any matter to be presented by a nominee stockholder at a shareholders meeting including any amendment affecting the voting and notice rights and obligations of nominee holders and associated persons who fail to make timely disclosures required by the U.S. Securities and Exchange Commission such as Schedule 13D.
9.	Where there are KMP(s) holding positions or serving as consultants for foreign person(s)	Any new positions held by persons required to be cleared in connection with the facility clearance. Excludes positions where the KMP is appointed by the U.S. parent business organization to a seat on the board or similar governing body of a foreign subsidiary, provided that the business organization promptly gives DSS notice of such appointment.
10.	Where there are any other factors of foreign person control or influence	Each change qualifying as an affirmative answer to this question and each change having a material effect on the ownership, control or influence of the business, operations, prospects, condition (financial or otherwise), or property of the business organization such that the security measures contemplated by an agreement with DoD to mitigate FOCI would not reasonably be expected to remove the possibility of unauthorized access to or adverse affect on the performance of classified contracts.

MATERIAL/SIGNIFICANT CHANGE GLOSSARY

Beneficial Ownership:

Beneficial ownership of securities means that a person has or shares the opportunity, directly or indirectly, to profit or share in any profit derived from a transaction in the securities, and includes the power to vote, direct the vote, dispose or direct to dispose such security.

Business Organization:

As used herein, "business organization" means the entity submitting the Material/Significant Change SF 328.

Indebtedness:

As used herein, "indebtedness" means its total liabilities, obligations and reserves, contingent or otherwise, which, in accordance with U.S. generally accepted accounting principles ("U.S. GAAP"), would be reflected as a liability on its balance sheet, including without limitation (i) any obligation for borrowed money or arising out of any credit facility, (ii) any obligation evidenced by bonds, debentures, notes or other similar instruments, (iii) any obligation to pay the deferred purchase price of property or services, (iv) any obligation under conditional sales or other title retention agreements, (v) the net aggregate rentals under any lease as lessee that under

U.S. GAAP would be capitalized on the books of the lessee or is the substantial equivalent of the financing of the property so leased, (vi) any obligation to purchase securities or other property which arises out of or in connection with the sale of the same or substantially similar securities or property or (vii) any instrument creating a mortgage, deed of trust, pledge, lien, security interest or other charge or encumbrance against any of its property, assets or leasehold interests.

Financial Statement

As used herein, "financial statements" means the business organization's most recent quarterly or annual balance sheet and statements of income, retained earnings, and sources and application of funds for such fiscal period, together with all notes thereto and with comparable figures for the corresponding period of its previous fiscal year, each prepared in U.S. dollars in accordance with U.S. GAAP.

Tangible Net Worth

As used herein, "tangible net worth" means, as of a stated date, (i) the total stockholders' equity (including capital stock, paid-in capital and retained earnings, after deducting treasury stock and reserves) that would appear on the business organization's financial statements prepared as of that date, less (ii) the aggregate book value of all intangible assets

shown on the business organization's financial statements as of that date (including, without limitation, goodwill, patents, trademarks, trade names, copyrights, franchises, and unrealized appreciation of assets).

h. Changes in Storage Capability. Any change in the storage capability that would raise or lower the level of classified information the facility is approved to safeguard.

i. Inability to Safeguard Classified Material. Any emergency situation that renders the facility incapable of safeguarding classified material.

j. Security Equipment Vulnerabilities. Significant vulnerabilities identified in security equipment, intrusion detection systems (IDS), access control systems, communications security (COMSEC) equipment or systems, and information system (IS) security hardware and software used to protect classified material.

k. Unauthorized Receipt of Classified Material. The receipt or discovery of any classified material that the contractor is not authorized to have. The report should identify the source of the material, originator, quantity, subject or title, date, and classification level.

l. Employee Information in Compromise Cases. When requested by the CSA, information concerning an employee when the information is needed in connection with the loss, compromise, or suspected compromise of classified information.

m. Disposition of Classified Material Terminated From Accountability. When the whereabouts or disposition of classified material previously terminated from accountability is subsequently determined.

n. Foreign Classified Contracts. Any precontract negotiation or award not placed through a GCA that involves, or may involve: (1) the release or disclosure of U.S. classified information to a foreign interest or (2) access to classified information furnished by a foreign interest.

1-303. Reports of Loss, Compromise, or Suspected Compromise. Any loss, compromise or suspected

compromise of classified information, foreign or domestic, shall be reported to the CSA. Classified material that cannot be located within a reasonable period of time shall be presumed to be lost until an investigation determines otherwise. If the facility is located on a Government installation, the report shall be furnished to the CSA through the Commander or Head of the host installation.

ISL 2006-02 #4 (1-302, 1-303, 1-304). Reports Submitted to the CSA (ISL 02L-1 #9). Reports of Loss, Compromise or Suspected Compromise in accordance with NISPOM Paragraph 1-303, will be submitted to the DSS Field Office.

ISL 2006-02 #5 (1-303 and 4-218). Notification to Recipients Regarding the Inadvertent Dissemination of Classified as Unclassified (ISL 00L-1 #8). Contractors are reminded that when classified information is transmitted or disseminated as unclassified, notification of the actual classification to recipients who are cleared for access to the material is, at a minimum, CONFIDENTIAL. Therefore, if the material was originally transmitted electronically, contractors must provide the classification notification via secure channels (e.g., cleared network, STU-III, secure fax). The notification should also provide the classification source as well as declassification instructions. When control of the material has been lost, or if unauthorized personnel have had access to the information, such as when the recipient is not cleared for access, the matter is to be reported to your DSS Field Office as a report of compromise. Regardless of whether the recipient is a cleared or uncleared contractor/individual, if the transmission occurred by an unsecure means, (i.e. unsecure fax, Internet, unclassified server, etc.), the control of the material is deemed lost.

a. Preliminary Inquiry. Immediately on receipt of a report of loss, compromise, or suspected compromise of classified information, the contractor shall initiate a preliminary inquiry to ascertain all of the circumstances surrounding the reported loss, compromise or suspected compromise.

b. Initial Report. If the contractor's preliminary inquiry confirms that a loss, compromise, or suspected compromise of any classified information occurred, the contractor shall promptly submit an

initial report of the incident unless otherwise notified by the CSA. Submission of the initial report shall not be deferred.

c. Final Report. When the investigation has been completed, a final report shall be submitted to the CSA. The report should include:

(1) Material and relevant information that was not included in the initial report;

(2) The name and social security number of the individual(s) who was primarily responsible for the incident, including a record of prior loss, compromise, or suspected compromise for which the individual had been determined responsible;

(3) A statement of the corrective action taken to preclude a recurrence and the disciplinary action taken against the responsible individual(s), if any; and conclusion that loss, compromise, or suspected compromise occurred or did not occur.

1-304. Individual Culpability Reports. Contractors shall establish and enforce policies that provide for appropriate administrative actions taken against

employees who violate requirements of this Manual. They shall establish and apply a graduated scale of disciplinary actions in the event of employee violations or negligence. A statement of the administrative actions taken against an employee shall be included in a report to the CSA when individual responsibility for a security violation can be determined and one or more of the following factors are evident:

ISL 2006-02 #4 (1-302, 1-303, 1-304). Reports Submitted to the CSA (ISL 02L-1 #9). Individual Culpability Reports in accordance with NISPOM Paragraph 1-304, will be submitted to DISCO.

a. The violation involved a deliberate disregard of security requirements.

b. The violation involved gross negligence in the handling of classified material.

c. The violation involved was not deliberate in nature but involves a pattern of negligence or carelessness.

CHAPTER 2 Security Clearances

Section 1. Facility Clearances (FCLs)

2-100. General. An FCL is an administrative determination that a company is eligible for access to classified information or award of a classified contract. Contract award may be made prior to the issuance of an FCL. In those cases, the contractor will be processed for an FCL at the appropriate level and must meet eligibility requirements for access to classified information. However, the contractor will not be afforded access to classified information until the FCL has been granted. The FCL requirement for a prime contractor includes those instances in which all classified access will be limited to subcontractors. Contractors are eligible for custody (possession) of classified material if they have an FCL and storage capability approved by the CSA.

a. An FCL is valid for access to classified information at the same or lower classification level as the FCL granted.

b. FCLs will be registered centrally by the U.S. Government.

c. A contractor shall not use its FCL for advertising or promotional purposes.

2-101. Reciprocity. An FCL shall be considered valid and acceptable for use on a fully reciprocal basis by all Federal departments and agencies, provided it meets or exceeds the level of clearance needed.

2-102. Eligibility Requirements. A contractor or prospective contractor cannot apply for its own FCL. A GCA or a currently cleared contractor may sponsor an uncleared company for an FCL. A company must meet the following eligibility requirements before it can be processed for an FCL:

ISL 2006-02 #6 (2-102 and 7-101). Facility Security Clearances (FCLs) for Service Contracts (ISL 05L-1 #8). DSS continues to receive requests to process companies for FCLs in order to perform service-oriented tasks (janitorial services for example). A fundamental requirement for FCL sponsorship is that the contractor must require access

to classified information in connection with a legitimate U.S. Government or foreign government procurement. A request to clear a company solely to avoid implementing basic security procedures that would otherwise preclude access to classified information (e.g., escort by an authorized person in combination with appropriate area sanitization), is not justification for an FCL, and could lead to security vulnerability.

There may be rare exceptions when a company would genuinely need an FCL to perform service-oriented tasks. An example is when a cleaning company is under contract to clean an area that, due to the nature of the classified material involved, cannot be adequately sanitized to preclude access to classified information even with appropriate escort. In those rare exceptions, the letter to DSS sponsoring the company for an FCL must clearly explain the rationale for the FCL. Such requests will be carefully scrutinized, and the validity for maintaining the FCL, once granted, will be a point of emphasis during recurring DSS security reviews.

ISL 2009-02 #1 (2-102). Eligibility of Companies Organized and Existing Under the Laws of U.S. Territories for Facility Clearances.

Q. NISPOM paragraph 2-102b. stipulates that a company must be organized and existing under the laws of any of the fifty states, the District of Columbia, or Puerto Rico, and be located in the United States or its territorial areas in order to be eligible for a facility clearance. What about companies that are organized and existing under the laws of other U.S. Territories?

A. The Department of Defense (DoD) examined the basis for this requirement, which has been DoD policy since 1974. Based on this review, the Department will not automatically exclude companies organized and existing under the laws of any of the organized United States territories (currently Guam, the Northern Marianas Islands, Puerto Rico and the U.S. Virgin Islands) from consideration for facility clearances. For purposes of

NISPOM paragraph 2-102b., the Defense Security Service (DSS) will process companies organized and existing under the laws of organized United States territories for a facility clearance, provided the company is also located in the United States or its Territorial Areas and is otherwise eligible for a facility clearance.

a. The company must need access to the classified information in connection with a legitimate U.S. Government or foreign government requirement.

b. The company must be organized and existing under the laws of any of the fifty states, the District of Columbia, or Puerto Rico, and be located in the United States or its territorial areas.

ISL 2013-01 (2-102.b.). Facility Clearance (FCL) Eligibility Requirements.

Background: National Industrial Security Program Operating Manual (NISPOM), paragraph 2-102b, stipulates that before being processed for an FCL, a company must be organized and existing under the laws of any of the 50 states, the District of Columbia, or Puerto Rico, and be located in the United States or its territorial areas in order to be eligible for an FCL. In Industrial Security Letter (ISL) 2009-02, June 6, 2009, DSS clarified that it will also process companies organized and existing under the laws of any of the organized U.S. territories (currently Guam, the Northern Marianas Islands, Puerto Rico and U.S. Virgin Islands) for an FCL provided such companies are located in the U.S. or its Territorial Areas and are otherwise eligible for a facility clearance.

To address FCL eligibility for the American Indian/Alaska Native tribal entities or those that are organized and existing under the laws of any of the Indian tribes, DSS will issue an FCL if they meet all of the following criteria in addition to meeting all other FCL requirements:

- The American Indian or Alaska Native tribe under whose laws the company is chartered must have been formally acknowledged by the Assistant Secretary - Indian Affairs, of the U.S. Department of the Interior, as a recognized American Indian or Alaska Native tribe.

- The company must have been organized, and continue to exist during the period of the FCL, under a tribal statute or code, or pursuant to a resolution of an authorized tribal legislative body.
- The company must submit records such as a charter, certificate of organization, or other applicable tribal documents and statute or code provisions governing the formation and continuation of the company, for a DSS determination that the company is tribally chartered as part of the FCL processing.

DSS will also process FCLs for federally-chartered tribal corporations formed under Section 17 of the Indian Reorganization Act (25 U.S.C. § 477) as well as for companies chartered under the laws of a U.S. state, the District of Columbia or an organized U.S. territory and owned in whole or in part by Indian tribes, provided they meet all other FCL eligibility criteria.

The NISPOM will be updated to include these FCL eligibility requirements.

c. The company must have a reputation for integrity and lawful conduct in its business dealings. The company and its key managers must not be barred from participating in U.S. Government contracts.

d. The company must not be under FOCI to such a degree that the granting of the FCL would be inconsistent with the national interest.

2-103. Processing the FCL. The CSA will advise and assist the company during the FCL process. As a minimum, the company will:

- a. Execute CSA-designated forms.
- b. Process key management personnel for PCLs.
- c. Appoint a U.S. citizen employee as the FSO.

2-104. PCLs Required in Connection with the FCL. The senior management official and the FSO must always be cleared to the level of the FCL. Other officials, as determined by the CSA, must be

granted PCLs or be excluded from classified access pursuant to paragraph 2-106.

2-105. PCLs Concurrent with the FCL. Contractors may designate employees who require access to classified information during the negotiation of a contract or the preparation of a bid or quotation pertaining to a prime contract or a subcontract to be processed for PCLs concurrent with the FCL. The granting of an FCL is not dependent on the clearance of such employees.

2-106. Exclusion Procedures. When, pursuant to paragraph 2-104, formal exclusion action is required, the organization's board of directors or similar executive body shall affirm the following, as appropriate.

a. Such officers, directors, partners, regents, or trustees (designated by name) shall not require, shall not have, and can be effectively excluded from access to all classified information disclosed to the organization. They also do not occupy positions that would enable them to adversely affect the organization's policies or practices in the performance of classified contracts. This action shall be made a matter of record by the organization's executive body. A copy of the resolution shall be furnished to the CSA.

b. Such officers or partners (designated by name) shall not require, shall not have, and can be effectively denied access to higher-level classified information (specify which higher level(s)) and do not occupy positions that would enable them to adversely affect the organization's policies or practices in the performance of higher-level classified contracts (specify higher level(s)). This action shall be made a matter of record by the organization's executive body. A copy of the resolution shall be furnished to the CSA.

2-107. Interim FCLs. An interim FCL may be granted to eligible contractors by the CSA. An interim FCL is granted on a temporary basis pending completion of the full investigative requirements.

2-108. Multiple Facility Organizations (MFOs). The home office facility must have an FCL at the same, or higher, level of any cleared facility within

the MFO. The CSA shall determine the necessity for branch offices to be cleared.

ISL 2006-02 #7 (2-108). Clearing Branch Offices (ISL 03L-1 #8). Historically, multiple facility organizations (MFOs) have had the option to centralize and administer certain security functions such as personnel clearance administration, security education, and classified visit authorizations within home office locations, or other cleared locations. Companies exercising this option maximize security resources and, in requiring fewer facility security clearances, avoid the related additional (processing and maintenance) costs by government and industry. There are currently numerous non-possessing division or branch offices cleared under the NISP. These are facilities that already have viable security programs established at their home office locations. Those home office locations can, in most cases, effectively administer the limited security administrative functions for these branch office locations. Accordingly, DSS will no longer process new facility security clearances (FCL) for division or branch offices that do not require possession of classified material for contract performance, unless there is a sufficient contractual or critical operational need.

Contractors considering administrative termination of non-possessing division or branch offices may contact their assigned DSS Industrial Security Representative for further guidance.

2-109. Parent-Subsidiary Relationships. When a parent-subsidiary relationship exists, the parent and the subsidiary will be processed separately for an FCL. As a general rule, the parent must have an FCL at the same, or higher, level as the subsidiary. However, the CSA will determine the necessity for the parent to be cleared or excluded from access to classified information. The CSA will advise the companies as to what action is necessary for processing the FCL. When a parent or its cleared subsidiaries are collocated, a formal written agreement to use common security services may be executed by the two firms, subject to the approval of the CSA.

2-110. Termination of the FCL. Once granted, an FCL remains in effect until terminated by either party. If the FCL is terminated for any reason, the

contractor shall return all classified material in its possession to the appropriate GCA or dispose of the material as instructed by the CSA.

2-111. Records Maintenance. Contractors shall maintain the original CSA designated forms for the duration of the FCL.

Section 2. Personnel Security Clearances

2-200. General

ISL 2006-01 #3 (2-200). Joint Personnel Adjudications System (JPAS). The Department of Defense has designated JPAS as its system of record for contractor eligibility and access to classified information. This means that JPAS is the “CSA-designated database” referenced in the revised NISPOM (paragraph 2-200b). Industry has been using JPAS since mid-2004. The first step for contractors using JPAS is to “take ownership” of their employees in the system. Guidance can be found in the “JCAVS Desktop Resource” on the JPAS Gateway website ([click here](#)) under the FAQs heading. Section #2 of the Desktop Resource explains “How to Establish a Personnel Security Management Network (PSM Net)”.

After almost 2 years of industry use of JPAS, a review of records in JPAS indicates over 18,000 contractor personnel whose records have no company affiliation. Contractors should ensure that all of their employees show their company/CAGE affiliation in the JPAS record. All unclaimed records will be purged from JPAS within the next year.

ISL 2006-01 #4 (2-200 and 2-211). Interim PCLs. The prohibition on eligibility for access to SAP and SCI information based on an interim PCL has been deleted. Eligibility for access to SCI and SAP information based on an interim PCL is a determination made by the granting authority.

ISL 2006-02 #8 (2-200). Personnel Security Clearances (PCLs), the Internet, and Job Seeking (ISL 03L-1 #13). The NISPOM clearly prohibits the use of a Facility Clearance for advertising purposes (2-100c, NISPOM). However, individuals may address specific qualification requirements associated with a position by informing prospective employers that they have been granted a PCL at the requisite level identified for the position. Aside from addressing specific qualifications for a particular position at a cleared contractor or Government facility, it is a poor security practice to identify oneself in a public database as a cleared person and become flagged as a possible target for foreign interests. Examples of such flagging, or identifying oneself as a cleared person, include online Internet

employment services that solicit clearance information as well as other personnel data, and make this publicly available by electronic means. It should be understood that the audience for the Internet is worldwide and includes a large number of domestic and foreign entities. Other examples of flagging are employment seminars or job fairs that invite only persons granted a clearance to attend and register. In general, these and similar situations may also provide opportunities for foreign targeting and collection efforts. Foreign entities may be interested in identifying individuals who access or can access classified information. It is recommended that persons granted a clearance should consider the prospective audience before identifying themselves as cleared.

a. An employee may be processed for a PCL when the contractor determines that access is essential in the performance of tasks or services related to the fulfillment of a classified contract. A PCL is valid for access to classified information at the same or lower level of classification as the level of the clearance granted.

b. The CSA will determine eligibility for access to classified information in accordance with the national standards and notify the contractor that eligibility has been granted. The CSA will notify the contractor when an employee's PCL has been denied, suspended, or revoked. The contractor shall immediately deny access to classified information to any employee when notified of a denial, revocation or suspension. When the CSA has designated a database as the system of record for contractor eligibility and access, the contractor shall be responsible for annotating and maintaining the accuracy of their employees' access records. Specific procedures will be provided by the CSA.

ISL 2010-01 #2 (2-200.b.). Security Management Office (SMO) Contact Information in JPAS. JPAS is the system of record for contractor eligibility and access to classified information for the Department of Defense. Within JPAS, each contractor's security office is represented by a SMO, which operates at a specified level and can be connected to other SMOs in ways that reflect real-world associations. The following is provided in

accordance with NISPOM paragraph 2-200b, which states that specific procedures for the use of the system of record will be provided by the cognizant security agency (CSA).

SMO Account Managers must update all SMO contact information in JPAS by March 31, 2010. The current SMO office name and other identifying characteristics (such as phone and fax numbers and email addresses) are necessary to help Government security managers and facility security officers (FSOs) locate and contact one another. Providing up-to-date email contact information is necessary to support future capabilities that will enable security officers to receive vital access and eligibility information without the need to be logged into JPAS.

The SMO Maintenance screen allows Account Managers to create, deactivate, and delete SMOs. It also allows Account Managers to update office information, view all associated users for a SMO and maintain its parental (superior) relationships. An Account Manager must have the proper user level and be within the same Service/Agency to establish and maintain a SMO. Within JPAS, the Joint Clearance Access and Verification System (JCAVS) tutorial link provides instructions for SMO Maintenance.

When creating and maintaining SMOs in JPAS, Account Managers must enter the email address and all contact information on the SMO Maintenance screen and must keep all contact information current. Account Managers may enter multiple email addresses in the email text box within the SMO Maintenance screen; however, it is important to enter only email addresses in this box (*separated by commas*) and not names or telephone numbers.

Procedures:

- Log in to JPAS/JCAVS as the “Account Manager”
- At the Main Menu, click on "Maintain Security Management Office"
- Enter the SMO Code in the “Search Criteria” box
- Click the SMO code link at the bottom of the window to select the SMO for maintenance

- The "Security Management Office Maintenance" screen is displayed. To update SMO Contact Information:
 - **"Commercial Phone" Text Box:** This is a required field. Enter the area code and phone number for a point of contact at the SMO.
 - **"Commercial Fax" Text Box:** Enter the area code and phone number for a fax number in service at the SMO.
 - **"Email" Text Box:** Enter the appropriate email address information for a point of contact at the SMO. **Multiple email addresses must be separated by a comma. Do not enter names or telephone numbers in this field.**
- Click the [SAVE] button

c. Within an MFO or within the same corporate family, contractors may centrally manage eligibility and access records.

d. The contractor shall limit requests for PCLs to the minimal number of employees necessary for operational efficiency, consistent with contractual obligations and other requirements of this Manual. Requests for PCLs shall not be made to establish "pools" of cleared employees.

e. The contractor shall not submit a request for a PCL to one agency if the employee applicant is cleared or is in process for a PCL by another agency. In such cases, to permit clearance verification, the contractor should provide the new agency with the full name, date and place of birth, social security number, clearing agency and type of investigation.

f. Access to SCI and SAP information is a determination made by the granting authority.

2-201. Investigative Requirements. Investigations conducted by a Federal agency shall not be duplicated by another Federal agency when those investigations are current within 5 years and meet the scope and standards for the level of PCL required. The types of investigations required are as follows:

ISL 2006-02 #9 (2-201). Interim Access to JPAS – Based on a National Agency Check (NAC) (ISL 03L-1 #11). The minimum requirement for access to the Joint Personnel Adjudication System (JPAS) is a clearance “eligibility” determination based on a

NACLC. The NACLC became the required investigative basis for all SECRET and CONFIDENTIAL clearances in January 1999. Therefore, some individuals requiring access to JPAS will have a SECRET or CONFIDENTIAL clearance based on a NAC. These individuals will be permitted interim access to JPAS provided they have submitted a request for a NACLC.

ISL 2006-02 #10 (2-201). Fingerprint Cards Not Required for Periodic Reinvestigations (ISL 05L-1 #7). It is no longer necessary to submit Fingerprint Cards (FPC) for any type of Periodic Reinvestigation (PR) unless specifically requested to do so. In the past, FPCs had to be submitted with requests for Secret and Confidential PRs but not Top Secret PRs.

a. Single Scope Background Investigation (SSBI). An SSBI is required for TOP SECRET, Q, and SCI access. Investigative requests shall be made using the electronic version of the Questionnaire for National Security Positions (SF 86).

b. National Agency Check with Local Agency Check and Credit Check (NACLC). An NACLC is required for a SECRET, L, and CONFIDENTIAL PCLs. Investigative requests shall be made using the electronic version of the SF 86.

c. Polygraph. Agencies with policies sanctioning the use of the polygraph for PCL purposes may require polygraph examinations when necessary. If issues of concern surface during any phase of security processing, coverage will be expanded to resolve those issues.

d. Reinvestigation. Contractor personnel may be subject to a reinvestigation program as specified by the CSA.

e. Financial Disclosure. When advised by the GCA that an employee is required to complete a Financial Disclosure Form, the contractor shall ensure that the employee has the opportunity to complete and submit the form in private.

2-202. Procedures for Completing the Electronic Version of the SF 86. The electronic version of the SF 86 shall be completed jointly by the employee and the FSO or an equivalent contractor employee(s) who

has (have) been specifically designated by the contractor to review an employee's SF 86.

ISL 2006-01 #5 (2-202). With the transition to e-QIP, industry has been unable to view the employee/applicant's SF 86 due to Privacy Act concerns. Now that industry is not reviewing the forms, the reject rate for e-QIP has gone up. Based on that information, a new procedure has been developed and industry will be able to review the forms with the April 2006 update to JPAS. The new procedures must be implemented before your company reviews employees' e-QIP submissions. The six month implementation for other provisions of the revised NISPOM does not apply for this particular requirement. Contractors that do not follow this procedure cannot review the employee/applicant SF 86 unless the employee/applicant has waived their right to privacy in writing.

The NISPOM revision requires that the facility security officer (FSO) and/or designee review the information on the SF 86 solely for completeness and not share the contents of the form with anyone else within the company. It requires written notification to the employee explaining the use of the information. Written notice can be as simple as giving the employee a copy of NISPOM paragraph 2-202. There is no requirement for the employee to certify that he/she has received this notification.

In most companies the FSO will be the reviewing official. Where this is not the case, particularly where a centralized personnel security clearance process has been established, either the corporate FSO or the FSO at the centralized location can designate personnel to do the review. It is not necessary for every contractor in the corporate family that uses a centralized process to specifically designate those persons to review the SF 86.

During security reviews, IS Reps will ask to speak to employees who recently completed their SF 86 to ensure that they received the required notice.

a. The FSO or designee shall inform the employee that the SF 86 is subject to review and shall review the application solely to determine its adequacy and to ensure that necessary information has not been omitted. The FSO or designee shall

provide the employee with written notification that review of the information is for adequacy and completeness, information will be used for no other purpose within the company, and that the information provided by the employee is protected by reference (I). The FSO or designee shall not share information from the employee's SF 86 within the company and shall not use the information for any purpose other than determining the adequacy and completeness of the SF 86.

b. The FSO or designee shall ensure that the applicant's fingerprints are authentic, legible, and complete to avoid subsequent clearance processing delays. The FSO or designee shall retain an original, signed copy of the SF 86, the Authorization for Release of Information and Records, and Authorization for Release of Medical Information until the clearance process has been completed. The FSO or designee shall maintain the retained documentation in such a manner that the confidentiality of the documents is preserved and protected against access by anyone within the company other than the FSO or designee. When the applicant's eligibility for access to classified information has been granted or denied, the retained documentation shall be destroyed.

2-203. Common Adjudicative Standards. Security clearance and SCI access determinations are based upon uniform common adjudicative standards.

2-204. Reciprocity. Federal agencies that grant access to classified information to their employees or their contractor employees are responsible for determining whether such employees have been previously cleared or investigated by the Federal Government. Any previously granted PCL that is based upon a current investigation of a scope that meets or exceeds that necessary for the clearance required shall provide the basis for issuance of a new clearance without further investigation or adjudication unless significant derogatory information that was not previously adjudicated becomes known to the granting agency.

2-205. Pre-employment Clearance Action. If access to classified information is required by a potential employee immediately upon commencement of their employment, a PCL application may be submitted to the CSA by the

contractor prior to the date of employment provided a written commitment for employment has been made by the contractor, and the candidate has accepted the offer in writing. The commitment for employment will indicate that employment shall commence within 30 days of the granting of eligibility for a PCL.

ISL 2009-02 #2 (2-205). In accordance with NISPOM paragraph 2-200a., contractor employees may be processed for a personnel security clearance (PCL) when access to classified information is essential for the performance of tasks or services related to the fulfillment of a classified contract. NISPOM 2-205 allows for submission of a PCL application prior to employment so long as a written commitment, indicating that employment must commence within 30 days of the granting of eligibility for the PCL, has been made to a prospective employee and the prospective employee has accepted that employment offer in writing. The prospective employee's PCL must be related to the fulfillment of a classified contract or other legitimate government requirement. The prospective employee must commence employment within 30 days of the granting of the eligibility, as annotated in JPAS, that permits the employee to perform the tasks or services associated with the contract or Government requirement for which the individual was hired.

As an example, if the duties of a specific contract on which the prospective employee is to perform require a final TOP SECRET (TS) eligibility, the contractor may defer the starting date of employment until the final TS eligibility has been granted, even if the prospective employee has an interim eligibility at any level or a final SECRET eligibility. Similarly, if the prospective employee requires a final SECRET eligibility in order to perform on a specific contract, the contractor may defer the starting date of employment until 30 days after the final SECRET eligibility is granted. If final eligibility is not required to perform on a contract, and the employee can perform the duties associated with the contract with an interim eligibility, then the employee must be on board within 30 days of the granting of the interim eligibility.

When a prospective employee has interim eligibility reflected in JPAS, but has not commenced employment, DSS may request documentation, such as the DD Form 254, from the contractor that

supports the contractor's determination that the individual cannot perform tasks or services without a final eligibility determination.

2-206. Contractor-Granted Clearances.

Contractors are no longer permitted to grant clearances. Contractor-granted CONFIDENTIAL clearances in effect under previous policy are not valid for access to RD, FRD, COMSEC information, SCI, NATO information (except RESTRICTED), and classified foreign government information (FGI), or for Critical or Controlled Nuclear Weapon Security positions.

2-207. Verification of U.S. Citizenship. The contractor shall require each applicant for a PCL who claims U.S. citizenship to produce evidence of citizenship.

2-208. Acceptable Proof of Citizenship

ISL 2010-01 #3 (2-208). In July 2008, the U.S. Department of State began issuing a Passport Card for entry by U.S. citizens into the U.S. from Canada, Mexico, and the countries of the Caribbean and Bermuda at land border crossings or sea ports-of-entry. The U.S. Passport Card, current or expired, is acceptable proof of U.S. citizenship for purposes of NISPOM paragraph 2-208.

ISL 2011-02 #1 (2-208). In December 2009, the government of Puerto Rico enacted a new law aimed at strengthening the issuance and usage of birth certificates to combat fraud and protect the identity and credit of all people born in Puerto Rico. The new law was based on collaboration with the U.S. Department of State and the U.S. Department of Homeland Security.

On July 1, 2010, Puerto Rico began issuing new birth certificates incorporating technology to limit the possibility of document forgery. The government of Puerto Rico extended the validity of expiring Puerto Rico birth certificates through October 30, 2010, as a transition period.

Contractors verifying citizenship of applicants who use a Puerto Rican birth certificate as proof of citizenship must verify that the birth certificate was issued on or after July 1, 2010. There is no requirement to re-verify citizenship for employees

who used a birth certificate from Puerto Rico as proof of U.S. citizenship prior to October 30, 2010.

For additional information, visit the Puerto Rico Federal Affairs Administration link below:
<http://www.prfaa.com/index.asp>.

a. For individuals born in the United States, a birth certificate is the primary and preferred means of citizenship verification. Acceptable certificates must show that the birth record was filed shortly after birth and it must be certified with the registrar's signature. It must bear the raised, impressed, or multicolored seal of the registrar's office. The only exception is if a State or other jurisdiction does not issue such seals as a matter of policy. Uncertified copies of birth certificates are not acceptable. A delayed birth certificate is one created when a record was filed more than one year after the date of birth. Such a certificate is acceptable if it shows that the report of birth was supported by acceptable secondary evidence of birth. Secondary evidence may include: baptismal or circumcision certificates, hospital birth records, or affidavits of persons having personal knowledge about the facts of birth. Other documentary evidence can be early census, school, or family bible records, newspaper files, or insurance papers. All documents submitted as evidence of birth in the U.S. shall be original or certified documents.

b. If the individual claims citizenship by naturalization, a certificate of naturalization is acceptable proof of citizenship.

c. If citizenship was acquired by birth abroad to a U.S. citizen parent or parents, the following are acceptable evidence:

(1) A Certificate of Citizenship issued by the Department of Homeland Security, U.S. Citizenship and Immigration Services (USCIS) or its predecessor organization.

(2) A Report of Birth Abroad of a Citizen of the United States of America

(3) A Certificate of Birth.

d. A passport, current or expired, is acceptable proof of citizenship.

e. A Record of Military Processing-Armed Forces of the United States (DD Form 1966) is acceptable proof of citizenship, provided it reflects U.S. citizenship.

2-209. Non-U.S. Citizens. Only U.S. citizens are eligible for a security clearance. Every effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to a non-U.S. citizen. Such individuals may be granted a Limited Access Authorization (LAA) in those rare circumstances where the non-U.S. citizen possesses unique or unusual skill or expertise that is urgently needed to support a specific U.S. Government contract involving access to specified classified information and a cleared or clearable U.S. citizen is not readily available. In addition, the LAA may be processed only with the concurrence of the GCA.

2-210. Access Limitations of an LAA. An LAA granted under the provisions of this Manual is not valid for access to the following types of information:

ISL 2006-02 #11 (2-210). An export authorization is required to release classified information to a non-U.S. citizen or intending citizen who has been issued a Limited Access Authorization (LAA). The LAA is a determination that the non-U.S. citizen or intending citizen is eligible to receive specified classified information. It cannot serve as an export authorization. Therefore, prior to submitting an application for an LAA to DISCO, the contractor must obtain a written disclosure determination from a principal or a designated disclosure official or obtain a State Department approved export license. This documentation must be submitted with the application for an LAA.

a. TOP SECRET information.

b. RD or FRD.

c. Information that has not been determined releasable by a U.S. Government designated disclosure authority to the country of which the individual is a citizen.

d. COMSEC information.

e. Intelligence information.

f. NATO Information. However, foreign nationals of a NATO member nation may be authorized access to NATO Information provided that: (1) A NATO Security Clearance Certificate is obtained by the CSA from the individual's home country; and (2) NATO access is limited to performance on a specific NATO contract.

g. Information for which foreign disclosure has been prohibited in whole or in part; and

h. Information provided to the U.S. Government in confidence by a third party government and classified information furnished by a third party government.

2-211. Interim PCLs. Applicants for TOP SECRET, SECRET, and CONFIDENTIAL PCLs may be routinely granted interim PCLs, as appropriate, provided there is no evidence of adverse information of material significance. The interim status will cease if results are favorable following completion of full investigative requirements. Non-U.S. citizens are not eligible for access to classified information on an interim basis.

ISL 2006-01 #4 (2-200 and 2-211). The prohibition on eligibility for access to SAP and SCI information based on an interim PCL has been deleted. Eligibility for access to SCI and SAP information based on an interim PCL is a determination made by the granting authority.

a. An interim SECRET or CONFIDENTIAL PCL is valid for access to classified information at the level of the eligibility granted, except for RD, COMSEC Information, and NATO information. An interim TOP SECRET PCL is valid for access to TOP SECRET information, RD, NATO Information, and COMSEC information at the SECRET and CONFIDENTIAL level. Access to SCI and SAP information based on an interim PCL is a determination made by the granting authority.

b. An interim PCL granted by the CSA negates any existing contractor-granted CONFIDENTIAL clearance. When an interim PCL has been granted and derogatory information is subsequently developed, the CSA may withdraw the interim

pending completion of the processing that is a prerequisite to the granting of a final PCL.

c. When an interim PCL for an individual who is required to be cleared in connection with the FCL is withdrawn, the individual must be removed from access or the interim FCL will also be withdrawn.

d. Withdrawal of an interim PCL is not a denial or revocation of the clearance and may not be appealed.

2-212. Consultants. A consultant is an individual under contract to provide professional or technical assistance to a contractor in a capacity requiring access to classified information. The consultant shall not possess classified material off the premises of the using (hiring) contractor except in connection with authorized visits. The consultant and the using contractor shall jointly execute a consultant certificate setting forth respective security responsibilities. The using contractor shall be the

consumer of the services offered by the consultant it sponsors for a PCL. For security administration purposes, the consultant shall be considered an employee of the using contractor. Consultants to GCAs shall be processed for PCLs by the GCA in accordance with GCA procedures.

ISL 2006-02 #12 (2-212). PCL/FCL Requirements for Self-Employed Consultants (ISL 03L-1 #6). Cleared contractors may process self-incorporated consultants for a PCL in accordance with NISPOM paragraph 2-213 provided the consultant and members of his/her immediate family are the sole owners of the consultant's company, and only the consultant requires access to classified information. In such cases, a facility security clearance (FCL) is not required. Should other employees of the consultant's company require access to classified information, it would constitute a classified subcontract, and as such, a DD Form 254 must be issued by the prime contractor, and the consultant's firm will require an FCL.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 3. Foreign Ownership, Control, or Influence (FOCI)

2-300. Policy. Foreign investment can play an important role in maintaining the vitality of the U.S. industrial base. Therefore, it is the policy of the U.S. Government to allow foreign investment consistent with the national security interests of the United States. The following FOCI policy for U.S. companies subject to an FCL is intended to facilitate foreign investment by ensuring that foreign firms cannot undermine U.S. security and export controls to gain unauthorized access to critical technology, classified information, and special classes of classified information.

a. A U.S. company is considered under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

b. Whenever a company has been determined to be under FOCI, the primary consideration shall be the safeguarding of classified information. The CSA is responsible for taking whatever interim action is necessary to safeguard classified information, in coordination with other affected agencies as appropriate.

c. A U.S. company determined to be under FOCI is ineligible for an FCL unless and until security measures have been put in place to negate or mitigate FOCI. When a contractor determined to be under FOCI is negotiating an acceptable FOCI mitigation/negation measure, an existing FCL shall continue so long as there is no indication that classified information is at risk of compromise. An existing FCL shall be invalidated if the contractor is unable or unwilling to negotiate an acceptable FOCI mitigation/negation measure. An existing FCL shall be revoked if security measures cannot be taken to remove the possibility of unauthorized access or adverse affect on classified contracts.

ISL 2009-02 #3 (2-300.c.). Negotiating an Acceptable FOCI mitigation measure.

Q: NISPOM paragraph 2-300c. states that an existing FCL shall be invalidated if the contractor is unable or unwilling to negotiate an acceptable FOCI mitigation measure. How does DSS determine that the contractor is unable or unwilling?

A: Ideally, the contractor will have an acceptable mitigation agreement in place prior to completion of the transaction (e.g., when the foreign interest assumes ownership of the cleared U.S. company). If there is not an acceptable measure in place when the transaction is completed, DSS must decide whether or not to invalidate the existing FCL. The critical determinant in this decision is the status of the FOCI mitigation when the transaction closes. As a general rule, DSS will invalidate the existing FCL at the completion of the transaction unless DSS determines that the contractor has submitted an acceptable FOCI action plan in accordance with paragraph 2-303.

Invalidation of the FCL renders a contractor ineligible to bid on new classified contracts or to receive new classified material except for information necessary for completion of essential contracts as determined by the government contracting activity (GCA).

d. If the company does not have possession of classified material, and does not have a current or impending requirement for access to classified information, the FCL shall be administratively terminated.

e. Changed conditions, such as a change in ownership, indebtedness, or the foreign intelligence threat, may justify certain adjustments to the security terms under which a company is operating or, alternatively, that a different FOCI negation method be employed. If a changed condition is of sufficient significance, it might also result in a determination that a company is no longer considered to be under FOCI or, conversely, that a company is no longer eligible for an FCL.

f. The Federal Government reserves the right and has the obligation to impose any security method, safeguard, or restriction it believes necessary to ensure that unauthorized access to classified information is effectively precluded and that

performance of classified contracts is not adversely affected.

g. Nothing contained in this section shall affect the authority of the Head of an Agency to limit, deny or revoke access to classified information under its statutory, regulatory or contract jurisdiction. For purposes of this section, the term "Agency" has the meaning provided at reference (h), to include the term "DoD Component."

2-301. Factors. The following factors relating to the company, the foreign interest, and the government of the foreign interest, as appropriate, shall be considered in the aggregate to determine whether an applicant company is under FOCI, its eligibility for an FCL, and the protective measures required:

a. Record of economic and government espionage against U.S. targets.

b. Record of enforcement and/or engagement in unauthorized technology transfer.

c. The type and sensitivity of the information that shall be accessed.

d. The source, nature and extent of FOCI, including whether foreign interests hold a majority or substantial minority position in the company, taking into consideration the immediate, intermediate, and ultimate parent companies. A minority position is deemed substantial if it consists of greater than 5 percent of the ownership interests or greater than 10 percent of the voting interest.

e. Record of compliance with pertinent U.S. laws, regulations and contracts.

f. The nature of any bilateral and multilateral security and information exchange agreements that may pertain.

g. Ownership or control, in whole or in part, by a foreign government.

2-302. Procedures. A company is required to complete a Certificate Pertaining to Foreign Interests when applying for an FCL or when significant changes occur to information previously submitted. In the case of a corporate family, the form shall be a

consolidated response rather than separate submissions from individual members of the corporate family.

ISL 2006-01 #6 (2-302). NISPOM paragraph 2-302 now states that "in the case of a corporate family, the form shall be a consolidated response rather than separate submissions from individual members of the corporate family." In the case of an organization with multiple tiers of parent-subsidary relationships, the SF 328 should be certified by the highest tier cleared entity. This would not preclude a subordinate entity from preparing the SF 328 as long as the top tier cleared entity certified the answers on the form. This principle applies equally to changed condition reports submitted in accordance with NISPOM paragraph 1-302g (5). Finally, please note that the requirement to update the form every five years has been eliminated. Reports are requested only when material changes to the previously submitted SF 328 occur.

ISL 2009-03 (1-302.g.(5) and 2-302).

Q: What constitutes a reportable material change under the National Industrial Security Program Operating Manual (NISPOM) paragraph 1-302.g.(5) or a reportable significant change under NISPOM paragraph 2-302?

A: While nothing in this ISL modifies the current reporting obligations, including but not limited to those under NISPOM paragraph 1-302.g.(1) through (4) or the rights of DoD to determine significance for purpose of NISPOM paragraph 2-300e, the following matrix describes circumstances that business organizations are required to report on the Standard Form 328, Certificate Pertaining to Foreign Interests, to the Defense Security Service (DSS). When submitting information, it is not necessary to repeat answers that have not changed. *(See Paragraph 1-302.(5) for the matrix.)*

a. If there are any affirmative answers on the Certificate Pertaining to Foreign Interests, or other information is received which indicates that the applicant company may be under FOCI, the CSA shall review the case to determine the relative significance of the information in regard to:

(1) Whether the applicant is under FOCI,

(2) The extent and manner to which the FOCI may result in unauthorized access to classified information or adversely impact classified contract performance; and

(3) The type of actions, if any, that would be necessary to negate the effects of FOCI to a level deemed acceptable to the Federal Government. Disputed matters may be appealed and the applicant shall be advised of the government's appeal channels by the CSA.

b. When a contractor with an FCL enters into negotiations for the proposed merger, acquisition, or takeover by a foreign interest, the contractor shall submit notification to the CSA of the commencement of such negotiations. The submission shall include the type of transaction under negotiation (stock purchase, asset purchase, etc.), the identity of the potential foreign interest investor, and a plan to negate the FOCI by a method outlined in 2-303. The company shall submit copies of loan, purchase and shareholder agreements, annual reports, bylaws, articles of incorporation, partnership agreements, and reports filed with other Federal agencies to the CSA.

c. When factors not related to ownership are present, positive measures shall assure that the foreign interest can be effectively mitigated and cannot otherwise adversely affect performance on classified contracts. Examples of such measures include modification or termination of loan agreements, contracts and other understandings with foreign interests; diversification or reduction of foreign-source income; demonstration of financial viability independent of foreign interests; elimination or resolution of problem debt; assignment of specific oversight duties and responsibilities to board members; formulation of special executive-level security committees to consider and oversee matters that affect the performance of classified contracts; physical or organizational separation of the contractor component performing on classified contracts; the appointment of a technology control officer; adoption of special Board Resolutions; and other actions that negate or mitigate foreign influence.

2-303. FOCI Action Plans. The following are the methods that can be applied to negate or mitigate the risk of foreign ownership or control.

ISL 2006-01 #7 (2-303). Access to proscribed information by a company cleared under a Special Security Agreement (SSA) may require that the GCA make a national interest determination (NID) that release of proscribed information to the company will not harm the national security interests of the United States. The preparation of the NID is the responsibility of the GCA. It is the responsibility of DSS to determine the need for a NID and to request the NID from the GCA. The determination of the need for a NID or its preparation is never the responsibility of the contractor.

If there is no indication to DSS that the GCA will decline to make the NID, DSS will not delay implementation of a FOCI action plan pending receipt of the NID from the GCA.

a. Board Resolution. When a foreign interest does not own voting interests sufficient to elect, or otherwise is not entitled to representation on the company's governing board, a resolution(s) by the governing board shall normally be adequate. The governing board shall identify the foreign shareholder and describe the type and number of foreign-owned shares; acknowledge the company's obligation to comply with all industrial security program and export control requirements; and certify that the foreign owner does not require, shall not have, and can be effectively precluded from unauthorized access to all classified and export-controlled information entrusted to or held by the company. The governing board shall provide for annual certifications to the CSA acknowledging the continued effectiveness of the resolution. The company shall distribute to members of its governing board and to its key management personnel copies of such resolutions, and report in the company's corporate records the completion of such distribution.

b. Voting Trust Agreement and Proxy Agreement. The Voting Trust Agreement and the Proxy Agreement are arrangements whereby the foreign owner relinquishes most rights associated with ownership of the company to cleared U.S. citizens approved by the U.S. Government. Under a Voting Trust Agreement, the foreign owner transfers legal title in the company to the Trustees. Under a Proxy Agreement, the foreign owner's voting rights are conveyed to the Proxy Holders. Neither arrangement imposes any restrictions on the

company's eligibility to have access to classified information or to compete for classified contracts.

(1) Establishment of a Voting Trust or Proxy Agreement involves the selection of Trustees or Proxy Holders, all of whom must become members of the company's governing board. Both arrangements must provide for the exercise of all prerogatives of ownership by the Trustees or Proxy Holders with complete freedom to act independently from the foreign owners, except as provided in the Voting Trust or Proxy Agreement. The arrangements may, however, limit the authority of the Trustees or Proxy Holders by requiring that approval be obtained from the foreign owner(s) with respect to matters such as:

- (a) The sale or disposal of the company's assets or a substantial part thereof;
- (b) Pledges, mortgages, or other encumbrances on the company's assets, capital stock or ownership interests;
- (c) Mergers, consolidations, or reorganizations;
- (d) Dissolution; and
- (e) Filing of a bankruptcy petition.

However, the Trustees or Proxy Holders may consult with the foreign owner, or vice versa, where otherwise consistent with U.S. laws, regulations and the terms of the Voting Trust or Proxy Agreement.

(2) The Trustees or Proxy Holders assume full responsibility for the foreign owner's voting interests and for exercising all management prerogatives relating thereto in such a way as to ensure that the foreign owner shall be insulated from the company, thereby solely retaining the status of a beneficiary. The company must be organized, structured, and financed so as to be capable of operating as a viable business entity independent from the foreign owner.

c. Special Security Agreement (SSA) and Security Control Agreement (SCA). The SSA and SCA are arrangements that, based upon an assessment of the FOCI factors, impose various

industrial security and export control measures within an institutionalized set of company practices and procedures. They require active involvement in security matters of senior management and certain Board members (outside directors), who must be cleared U.S. citizens; provide for the establishment of a Government Security Committee (GSC) to oversee classified and export control matters; and preserve the foreign owner's right to be represented on the Board (inside directors) with a direct voice in the business management of the company while denying unauthorized access to classified information.

(1) When a company is not effectively owned or controlled by a foreign interest and the foreign interest is nevertheless entitled to representation on the company's governing board, the company may be cleared under an SCA. There are no access limitations under an SCA.

(2) A company that is effectively owned or controlled by a foreign interest may be cleared under an SSA arrangement. Access to proscribed information¹ by a company cleared under an SSA may require that the GCA complete a National Interest Determination (NID) to determine that release of proscribed information to the company shall not harm the national security interests of the United States. The CSA shall advise the GCA on the need for a NID.

¹ Proscribed information includes TS, COMSEC except classified keys used for data transfer, RD as defined in reference (c), SAP, and SCI.

ISL 2011-02 #2 (2-303.c.(2)). Communications Security (COMSEC) and Proscribed Information.

Question: In the context of National Industrial Security Program Operating Manual (NISPOM) paragraph 2-303.c.(2), when is COMSEC material considered proscribed information?

Answer: All COMSEC material is proscribed information except for Controlled Cryptographic Items when unkeyed or utilized with unclassified keys.

Background:

In accordance with NISPOM paragraph 2-303.c.(2), companies cleared under Special Security Agreements (SSAs) require National Interest Determinations (NIDs) in order to perform on contracts requiring access to proscribed information. The current version of the NISPOM defines the COMSEC category of proscribed information as “COMSEC, except classified keys used for data transfer.”

Unfortunately, this definition is ambiguous and has created confusion. To some contractor personnel and government officials, the current wording suggests that all COMSEC hardware (even unclassified Controlled Cryptographic Items) is proscribed information while even the most sensitive classified keys are not. This is not the intended interpretation.

To address the ambiguity and to resolve any confusion, the Department of Defense (DoD) has issued the following revised definition of proscribed information to DoD Government Contracting Activities and to the 23 non-DoD agencies receiving DoD industrial security services. This clarification reflects current DoD policies and practices and will be incorporated into the next revision to the NISPOM.

Proscribed information includes Top Secret (TS); COMSEC material, excluding Controlled Cryptographic Items when unkeyed or utilized with unclassified keys; Restricted Data (RD); Special Access Program (SAP); and Sensitive Compartmented Information (SCI). Access to the proscribed information in this subparagraph shall not be granted without the approval of the agency with control jurisdiction (e.g., National Security Agency (NSA) for COMSEC, whether the COMSEC is proscribed information or not; the Office of the Director of National Intelligence (ODNI) for SCI; and Department of Energy (DOE) for RD) in accordance with its policies.

NSA will (as stated in NISPOM 9-401) continue to establish specific requirements for the management and safeguarding of COMSEC materials in industry. In addition, NSA approval will be required before access to COMSEC can be granted, regardless of

whether the COMSEC information is proscribed or classified information and whether or not there is a Foreign Ownership, Control or Influence mitigation agreement in place.

(a) The NID can be program, project or contract specific. A separate NID is not required for each contract under a program or project. The NID decision shall be made at the GCA’s Program Executive Office level. If the proscribed information is under the classification or control jurisdiction of another agency, the GCA shall advise that agency; e.g., National Security Agency (NSA) for COMSEC, DNI for SCI, DOE for RD. These agencies may determine that release to the contractor of an entire category of information under their control may not harm the national security.

(b) The GCA shall forward the completed NID to the CSA. The CSA shall not delay implementation of a FOCI action plan pending completion of a GCA’s NID process as long as there is no indication that a NID shall be denied.

2-304. Citizenship of Persons Requiring PCLs. Under all methods of FOCI mitigation or negation, management positions requiring PCLs in conjunction with the FCL must be filled by U.S. citizens residing in the United States.

2-305. Qualifications of Trustees, Proxy Holders, and Outside Directors. Individuals who serve as Trustees, Proxy Holders, or Outside Directors must be:

a. Resident U.S. citizens who can exercise management prerogatives relating to their position in a way that ensures that the foreign owner can be effectively insulated from the company;

b. Except as approved by the CSA in advance and in writing, completely disinterested individuals with no prior involvement with the company, the entities with which it is affiliated, or the foreign owner; and

c. Issued a PCL at the level of the facility’s FCL.

2-306. GSC. Under a Voting Trust, Proxy Agreement, SSA and SCA, the contractor is required

to establish a permanent committee of its Board of Directors, known as the GSC.

a. Unless otherwise approved by the CSA, the GSC consists of Voting Trustees, Proxy Holders or Outside Directors, as applicable, and those officers/directors who hold PCLs.

b. The members of the GSC are required to ensure that the contractor maintains policies and procedures to safeguard classified and export controlled information entrusted to it, and that violations of those policies and procedures are promptly investigated and reported to the appropriate authority when it has been determined that a violation has occurred.

c. The GSC shall also take the necessary steps to ensure that the contractor complies with U.S. export control laws and regulations and does not take action deemed adverse to performance on classified contracts. This shall include the appointment of a Technology Control Officer (TCO) and the establishment of Technology Control Plan (TCP).

d. The contractor's FSO shall be the principal advisor to the GSC and attend GSC meetings. The Chairman of the GSC must concur with the appointment and replacement of FSOs selected by management. The FSO and TCO functions shall be carried out under the authority of the GSC.

2-307. TCP. A TCP approved by the CSA shall be developed and implemented by those companies cleared under a Voting Trust Agreement, Proxy Agreement, SSA and SCA and when otherwise deemed appropriate by the CSA. The TCP shall prescribe all security measures determined necessary to reasonably foreclose the possibility of inadvertent access by non-U.S. citizen employees and visitors to information for which they are not authorized. The TCP shall also prescribe measures designed to assure that access by non-U.S. citizens is strictly limited to only that specific information for which appropriate Federal Government disclosure authorization has been obtained; e.g., an approved export license or technical assistance agreement. Unique badging, escort, segregated work area, security indoctrination schemes, and other measures shall be included, as appropriate.

2-308. Annual Review and Certification

a. Annual Review. The CSA shall meet at least annually with the GSCs of contractors operating under a Voting Trust, Proxy Agreement, SSA, or SCA to review the purpose and effectiveness of the clearance arrangement and to establish common understanding of the operating requirements and their implementation. These reviews shall also include an examination of the following:

(1) Acts of compliance or noncompliance with the approved security arrangement, standard rules, and applicable laws and regulations;

(2) Problems or impediments associated with the practical application or utility of the security arrangement; and

(3) Whether security controls, practices, or procedures warrant adjustment.

b. Annual Certification. For contractors operating under a Voting Trust Agreement, Proxy Agreement, SSA or SCA, the Chairman of the GSC shall submit to the CSA one year from the effective date of the agreement and annually thereafter an implementation and compliance report. Such reports shall include the following:

(1) A detailed description of the manner in which the contractor is carrying out its obligations under the agreement;

(2) Changes to security procedures, implemented or proposed, and the reasons for those changes;

(3) A detailed description of any acts of noncompliance, whether inadvertent or intentional, with a discussion of steps that were taken to prevent such acts from recurring;

(4) Any changes, or impending changes, of key management personnel or key board members, including the reasons therefore;

(5) Any changes or impending changes in the organizational structure or ownership, including any acquisitions, mergers or divestitures; and

(6) Any other issues that could have a bearing on the effectiveness of the applicable agreement.

2-309. Limited FCL. The United States has entered into Industrial Security Agreements with certain foreign governments. Some of these agreements establish arrangements whereby a foreign-owned U.S. company may be considered eligible for an FCL without any additional FOCI negation or mitigation instrument. Access limitations are inherent with the granting of Limited FCLs and are imposed upon all of the company's employees regardless of citizenship.

a. A Limited FCL may be granted upon satisfaction of the following criteria:

(1) There is an Industrial Security Agreement with the foreign government of the country from which the foreign ownership is derived.

(2) Release of classified information is in conformity with the U.S. National Disclosure Policy. Key management personnel may be citizens of the country of ownership for whom the United States has obtained security assurances at the appropriate level.

b. In extraordinary circumstances, a Limited FCL may also be granted even if the above criteria cannot be satisfied if there is a compelling need to do so consistent with U.S. national security interests. In any such case, the GCA shall provide a compelling need statement to the CSA to justify the FCL and verify that access to classified information is essential for contract performance. The CSA shall acknowledge the existence of a Limited FCL only to that GCA.

2-310. Foreign Mergers, Acquisitions and Takeovers, and the Committee on Foreign Investment in the United States (CFIUS)

a. The CFIUS, an interagency committee chaired by the Treasury Department, conducts reviews of proposed mergers, acquisition or takeovers of U.S. persons by foreign interests under section 721 (Exon-Florio amendment) of the Defense Production Act (reference (m)). CFIUS review is a voluntary process and affords an opportunity to foreign persons and U.S. persons entering into a covered transaction to submit the transaction for review by CFIUS to assess the impact of the transaction on U.S. national security.

b. The CFIUS review and the CSA industrial security FOCI review are carried out in two parallel but separate processes with different time constraints and considerations.

c. If a transaction under CFIUS review would require FOCI negation or mitigation measures if consummated, the CSA shall promptly advise the parties to the transaction and request that they submit to the CSA a plan to negate or mitigate FOCI. If it appears that an agreement cannot be reached on material terms of a FOCI action plan, or if the U.S. party to the proposed transaction fails to comply with the FOCI reporting requirements of this Manual, the CSA may recommend a full investigation of the transaction by CFIUS to determine the effects on national security.

d. If the CSA becomes aware of a proposed transaction that should be reviewed by CFIUS, and the parties thereto do not file a joint voluntary notice with CFIUS to initiate review within a reasonable time, the CSA shall initiate action to have CFIUS notified.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

CHAPTER 3 Security Training and Briefings

Section 1. Security Training and Briefings

3-100. General. Contractors shall provide all cleared employees with security training and briefings commensurate with their involvement with classified information.

3-101. Training Materials. Contractors may obtain defensive security, threat awareness, and other education and training information and material from their CSA or other sources.

3-102. FSO Training. Contractors shall be responsible for ensuring that the FSO, and others performing security duties, complete security training considered appropriate by the CSA. Training requirements shall be based on the facility's involvement with classified information and may include an FSO orientation course and for FSOs at facilities with safeguarding capability, an FSO Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of FSO.

ISL 2012-03 (3-102) NISPOM paragraph 3-102 requires contractors to ensure facility security officers (FSOs) and other contractor personnel performing security duties complete security training considered appropriate by the Cognizant Security Agency (CSA). The guidance in this ISL replaces the guidance previously published by the Defense Security Service (DSS) in Article 4 of ISL 2010-01, which is hereby cancelled.

In an effort to help contractors identify training requirements based on a facility's involvement with classified information, the DSS Center for Development of Security Excellence (CDSE) has created curricula that meet the FSO orientation and FSO program management course requirements referenced in the NISPOM paragraph 3-102.

Training to meet the orientation course requirements is in CDSE's FSO Curriculum for Non-Possessing Facilities. Training to meet the program management course requirements is in CDSE's FSO Curriculum for Possessing Facilities. Please refer to the CDSE website at

<http://www.dss.mil/cdse/catalog/curricula/index.html> for a description of the courses and examinations comprising the FSO curricula.

Successful completion of any of the previous versions of FSO training provided by CDSE, the DSS Academy, or the Department of Defense Security Institute satisfies the current NISPOM requirement unless advised otherwise by DSS.

3-103. Government-Provided Briefings. The CSA is responsible for providing initial security briefings to the FSO and for ensuring that other briefings required for special categories of information are provided.

3-104. Temporary Help Suppliers. A temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, shall be responsible for ensuring that required briefings are provided to their cleared personnel. The temporary help supplier or the using contractor may conduct these briefings.

3-105. Classified Information Nondisclosure Agreement (SF 312). The SF 312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial PCL must execute an SF 312 prior to being granted access to classified information. The contractor shall forward the executed SF 312 to the CSA for retention. If the employee refuses to execute the SF 312, the contractor shall deny the employee access to classified information and submit a report to the CSA. The SF 312 shall be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date.

ISL 2006-02 #13 (3-105). SF 312 Date in JPAS (ISL 05L-1 #6). Personnel records in JPAS often contain a date for the Classified Information Nondisclosure Agreement (SF 312). The date reflected is normally the day the SF 312 was entered by DISCO in the system, not the date the SF 312 was signed. It is very important that this date not be

changed in JPAS. The filing system DISCO uses to enable retrieval of the SF 312s is based on the date the SF 312 was processed by DISCO. As such, changing the date in JPAS would make it nearly impossible to locate a SF 312 should it be necessary.

Contractors are now responsible for entering this date in JPAS prior to granting the employee access to classified information. If a contractor is entering the SF 312 date, it should be the date the employee signed the form. If there is already a signed SF 312 on file for the employee as noted in JPAS, the employee is not required to sign another SF 312.

ISL 2006-02 #14 (3-105). Q&A – SF-312 (ISL 02L-1 #18).

Question: Is the Facility Security Officer (FSO) the only facility employee that can sign the acceptance block on the SF 312?

Answer: No. In accordance with “Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet”, dated Spring 2001, “an authorized representative of a contractor, licensee, grantee, or other non-Government organization acting as a designated agent of the United States Government is empowered to witness the execution of the SF 312 by another non-Government employee, and may accept it on behalf of the United States”. In most cases, authorized representatives of a contractor would be the FSO, other security officials under the oversight of the FSO, or one of the KMPs (Key Management Personnel).

3-106. Initial Security Briefings. Prior to being granted access to classified information, an employee shall receive an initial security briefing that includes the following:

- a. A threat awareness briefing.
- b. A defensive security briefing.
- c. An overview of the security classification system.
- d. Employee reporting obligations and requirements.
- e. Security procedures and duties applicable to the employee's job.

3-107. Refresher Training. The contractor shall provide all cleared employees with some form of security education and training at least annually. Refresher training shall reinforce the information provided during the initial security briefing and shall keep cleared employees informed of appropriate changes in security regulations. Training methods may include group briefings, interactive videos, dissemination of instructional materials, or other media and methods. Contractors shall maintain records about the programs offered and employee participation in them. This requirement may be satisfied by use of distribution lists, facility/department-wide newsletters, or other means acceptable to the FSO.

3-108. Debriefings. Contractors shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's PCL is terminated, suspended, or revoked; and upon termination of the FCL.

CHAPTER 4 Classification and Marking

Section 1. Classification

ISL 2013-06 31 (Chapter 4). Derivative Classification Responsibilities. On March 28, 2013, the Department of Defense released Conforming Change 1 to DoD 5220.22-M, "National Industrial Security Manual Operating Manual (NISPOM)."¹ This Industrial Security Letter (ISL) provides clarification to contractors for specific NISPOM paragraphs in Chapter 4 related to derivative classification. Contractors must ensure that all personnel who perform duties as derivative classifiers complete training by December 31, 2013. DSS will assess contractor compliance with derivative classification responsibilities after that date.

¹ summary of changes in Conforming Change 1 to the NISPOM:
http://www.dtic.mil/whs/directives/corres/pdf/522022m_summaryofchanges.pdf

4-100. General. Information is classified under reference (b) by an original classification authority and is designated and marked as TOP SECRET, SECRET, or CONFIDENTIAL. The designation UNCLASSIFIED is used to identify information that does not require a security classification. Except as provided by statute, no other terms may be used to identify classified information.

4-101. Original Classification. An original classification decision at any level can be made only by a U.S. Government official who has been designated or delegated the authority in writing. A determination to originally classify information may be made only when (a) an original classification authority is classifying the information; (b) the information falls into one or more of the categories set forth in reference (b); (c) the unauthorized disclosure of the information, either by itself or in context with other information, reasonably could be expected to cause damage to the national security, which includes defense against transnational terrorism, that can be identified or described by the original classifier; and (d) the information is owned by, produced by or for, or is under the control of the U. S. Government. The original classifier must state the concise "Reason" for classification on the front of

the document. The original classifier must also indicate either a date or event for the duration of classification for up to 10 years from the date of the original classification decision unless the date is further extended due to information sensitivities for up to 25 or 50 years.

4-102. Derivative Classification Responsibilities

a. Contractor personnel make derivative classification decisions when they incorporate, paraphrase, restate, or generate in new form, information that is already classified; then mark the newly developed material consistently with the classification markings that apply to the source information.

b. Derivative classification includes the classification of information based on guidance, which may be either a source document or classification guide. The duplication or reproduction of existing classified information is not derivative classification.

c. Classified information in e-mail messages is subject to all requirements of reference (b) and Part 2001 of Title 32, CFR, current editions, (reference (z)). If an e-mail is transmitted on a classified system, includes a classified attachment and contains no classified information within the body of the e-mail itself, then the e-mail is not a derivative classification decision. The e-mail overall classification must reflect the highest level present in the attachment.

d. The contractor shall ensure that all employees authorized to make derivative classification decisions:

ISL 2013-06 #2 (4-102.d.). Identification of authorized derivative classifiers. Contractors must ensure that all contractor cleared personnel authorized to make derivative classification decisions are identified on the documents on which they make derivative classification decisions. Please note that this includes contractor cleared personnel who

derivatively classify e-mail. Unless otherwise directed by a government customer, contractors have the option to use name and position or a personal identifier as the identification for the contractor's cleared personnel who are authorized to make derivative classification decisions, in accordance with the provisions of NISPOM paragraph 4-208.

Several examples of how a contractor may implement the requirements are: when contractors choose to have their cleared personnel use personal identifiers in lieu of name and position, the individual personal identifier would be unique, and could be linked to the derivative classifier on a list or roster maintained by the contractor for at least the duration of the individual's employment at the contractor or with the business organization of which the contractor is a part. A business organization¹ may also maintain such a roster for the entire organization.

¹ Business organization: a legal entity, such as a corporation, its subsidiaries, divisions and branch offices.

(1) Are identified by name and position, or by personal identifier, on documents they derivatively classify.

(2) Observe and respect original classification decisions.

(3) Carry forward the pertinent classification markings to any newly created documents. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(a) The date or event for declassification that corresponds to the longest period of classification among the sources; and

(b) A listing of the source materials.

(4) Are trained, in accordance with CSA direction, in the proper application of the derivative classification principles, with an emphasis on avoiding over-classification, at least once every 2 years. Training will cover classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

(5) Are not authorized to conduct derivative classification until they receive such training.

(6) Are given ready access to the pertinent classification guides and/or guidance necessary to fulfill these important actions.

e. Whenever practicable, derivative classifiers shall use a classified addendum if classified information constitutes a small portion of an otherwise unclassified document.

4-103. Security Classification Guidance. The GCA is responsible for incorporating appropriate security requirements clauses in a classified contract, Invitation for Bid (IFB), Request for Proposal (RFP), Request for Quotation (RFQ), or other solicitation, and for providing the contractor with the security classification guidance needed during the performance of the contract. This guidance is provided to the contractor by the Contract Security Classification Specification. The Contract Security Classification Specification must identify the specific elements of classified information involved in the contract that require security protection.

a. Contractors shall, to the extent practicable, advise and assist in the development of the original Contract Security Classification Specification. It is the contractor's responsibility to understand and apply all aspects of the classification guidance. Users of classification guides are also encouraged to notify the originator of the guide when they acquire information that suggests the need for change in the instructions contained in the guide. Classification guidance is, notwithstanding the contractor's input, the exclusive responsibility of the GCA, and the final determination of the appropriate classification for the information rests with that activity. The Contract Security Classification Specification is a contractual specification necessary for performance on a classified contract. If a classified contract is received without a Contract Security Classification Specification, the contractor shall advise the GCA.

b. The GCA is required to review the existing guidance periodically during the performance stages of the contract and to issue a revised Contract Security Classification Specification when a change occurs to the existing guidance or when additional

security classification guidance is needed by the contractor.

c. Upon completion of a classified contract, the contractor must dispose of the classified information according to Chapter 5, Section 7. If the GCA does not advise to the contrary, the contractor may retain classified material for a period of 2 years following completion of the contract. The Contract Security Classification Specification will continue in effect for this 2-year period. If the GCA determines the contractor has a continuing need for the material, the GCA must issue a final Contract Security Classification Specification for the classified contract. A final specification is provided to show the retention period and to provide final disposition instructions for the classified material under the contract.

4-104. Challenges to Classification. Should a contractor believe (a) that information is classified improperly or unnecessarily; or (b) that current security considerations justify downgrading to a lower classification or upgrading to a higher classification; or (c) that the security classification guidance is improper or inadequate, the contractor shall discuss such issues with the pertinent GCA for remedy. If a solution is not forthcoming, and the contractor believes that corrective action is still required, a formal written challenge shall be made to the GCA. Such challenges shall include a description sufficient to identify the issue, the reasons why the contractor believes that corrective action is required, and any recommendations for appropriate corrective action. In any case, the information in question shall be safeguarded as required by this Manual for its assigned or proposed level of classification, whichever is higher, until action is completed. If no written answer is received within 60 days, the CSA should be requested to provide assistance in obtaining a response. If no response is received from the GCA within 120 days, the contractor may also forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP) through the ISOO. The fact that a contractor has initiated such a challenge will not, in any way, serve as a basis for adverse action by the Government. If a contractor believes that adverse action did result from a classification challenge, full details should be furnished promptly to the ISOO for resolution.

4-105. Contractor Developed Information.

Whenever a contractor develops an unsolicited proposal or originates information not in the performance of a classified contract, the following rules shall apply:

a. If the information was previously identified as classified, it shall be classified according to an appropriate Contract Security Classification Specification, classification guide, or source document, and marked as required by this Chapter.

b. If the information was not previously classified, but the contractor believes the information may or should be classified, the contractor should protect the information as though classified at the appropriate level and submit it to the agency that has an interest in the subject matter for a classification determination. In such a case, the following marking, or one that clearly conveys the same meaning, may be used:

CLASSIFICATION DETERMINATION PENDING
Protect as though classified (TOP SECRET,
SECRET, or CONFIDENTIAL).

This marking shall appear conspicuously at least once on the material but no further markings are necessary until a classification determination is received. In addition, contractors are not precluded from marking such material as company-private or proprietary information. Pending a final classification determination, the contractor should protect the information. It should be noted however, that reference (b) prohibits classification of information over which the Government has no jurisdiction. To be eligible for classification, the information must: (1) incorporate classified information to which the contractor was given prior access, or (2) the Government must first acquire a proprietary interest in the information.

4-106. Classified Information Appearing in Public Media.

The fact that classified information has been made public does not mean that it is automatically declassified. Contractors shall continue the classification until formally advised to the contrary. Questions about the propriety of continued classification in these cases should be brought to the immediate attention of the GCA.

4-107. Downgrading or Declassifying Classified Information. Information is downgraded or declassified based on the loss of sensitivity of the information due to the passage of time or on occurrence of a specific event. Contractors downgrade or declassify information based on the guidance provided in a Contract Security Classification Specification or upon formal notification. If material is marked for automatic declassification, the contractor shall seek guidance from the GCA prior to taking any action. Downgrading or declassifying actions constitute implementation of a directed action rather than an exercise of the authority for deciding the change or cancellation of the classification. At the time the material is actually downgraded or declassified, the action to update records and change the classification markings shall be initiated and performed. Declassification is not automatically an approval for public disclosure.

ISL 2006-01 #8 (4-107 and 4-216.a.). Material Marked for Automatic Declassification. The term “automatic” declassification would seem to indicate that when classified material is marked with a declassification date, the contractor is authorized to automatically declassify the document. However, certain government agencies are concerned that, with all of the changes that have occurred to the declassification policy over the years, information may still retain sensitivity and therefore should not be “automatically” declassified.

When the contractor has material marked for automatic declassification, and notes that the date or event for the automatic declassification has occurred, the contractor must seek guidance from the government activity that released the information using the procedures of NISPOM paragraph 4-104. In effect, contractors are not authorized to unilaterally declassify even when the material is marked for automatic declassification.

Section 2. Marking Requirements

4-200. General. Physically marking classified information with appropriate classification markings serves to warn and inform holders of the information of the degree of protection required. Other notations facilitate downgrading, declassification, and aid in derivative classification actions. Therefore, it is essential that all classified information and material be marked to clearly convey to the holder the level of classification assigned, the portions that contain or reveal classified information, the period of time protection is required, the identity (by name and position or personal identifier) of the classifier, the source(s) for derivative classification, and any other notations required for protection of the information.

4-201. Marking Requirements for Information and Material. As a general rule, the markings specified in paragraphs 4-202 through 4-208 are required for all classified information regardless of the form in which it appears. Some material, such as documents, letters, and reports, can be easily marked with the required markings. Marking other material, such as equipment, IS media, and slides may be more difficult due to size or other physical characteristics. Since the primary purpose of the markings is to alert the holder that the information requires special protection, it is essential that all classified material be marked to the fullest extent possible to ensure the necessary safeguarding.

4-202. Identification Markings. All classified material shall be marked to show the name and address of the contractor responsible for its preparation, the identity of the person (by name and position or personal identifier) responsible for each derivative classification action, and the date of preparation. These markings are required on the face of all classified documents.

4-203. Overall Markings. The highest level of classified information contained in a document is its overall marking. The overall marking shall be conspicuously marked or stamped at the top and bottom on the outside of the front cover, on the title page, on the first page, and on the outside of the back. All copies of classified documents shall also bear the required markings. Overall markings shall be stamped, printed, etched, written, engraved, painted, or affixed by means of a tag, sticker, decal,

or similar device on classified material other than documents, and on containers of such material, if possible. If marking the material or container is not practical, written notification of the markings shall be furnished to recipients.

4-204. Page Markings. Interior pages of classified documents shall be conspicuously marked or stamped at the top and bottom with the highest classification of the information appearing thereon, or the designation UNCLASSIFIED, if all the information on the particular page is UNCLASSIFIED. Alternatively, the overall classification of the document may be conspicuously marked or stamped at the top and bottom of each interior page, when necessary to achieve production efficiency, and the particular information to which classification is assigned is adequately identified by portion markings according to paragraph 4-206.

4-205. Component Markings. The major components of complex documents are likely to be used separately. In such cases, each major component shall be marked as a separate document. Examples include: (a) each annex, appendix, or similar component of a plan, program, or project description; (b) attachments and appendices to a letter; and (c) each major part of a report. If an entire major component is UNCLASSIFIED, the first page of the component may be marked at the top and bottom with the designation UNCLASSIFIED and a statement included, such as: "All portions of this (annex, appendix, etc.) are UNCLASSIFIED." When this method of marking is used, no further markings are required on the unclassified major component.

4-206. Portion Markings.

a. Each section, part, paragraph, or similar portion of a document containing classified information shall be marked to show the highest level of its classification, or that the portion is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contain or reveal classified information. Classification levels of portions of a document shall be shown by the appropriate classification symbol placed immediately before the portion to which it applies. For paragraphs or subparagraphs beginning

with numbers, letters or symbols such as bullets, place the portion marking after the number, letter or bullet and before the text. In marking portions, the parenthetical symbols (TS) for TOP SECRET, (S) for SECRET, (C) for CONFIDENTIAL, and (U) for UNCLASSIFIED shall be used.

b. Illustrations, photographs, figures, graphs, drawings, charts, or similar portions contained in classified documents shall be marked clearly to show their classified or unclassified status. These classification markings shall not be abbreviated and shall be prominent and placed within or contiguous to such a portion. Captions of such portions shall be marked on the basis of their content.

4-207. Subject and Title Markings. Unclassified subjects and titles shall be selected for classified documents, if possible. A subject or title shall be marked with the appropriate symbol placed immediately before the item, which shall reflect the classification of the title, not the content of the document.

4-208. Markings for Derivatively Classified Documents. All classified information shall be marked to reflect the source of the classification and declassification instructions. Documents shall show the required information either on the cover, first page, title page, or in another prominent position. Other material shall show the required information on the material itself or, if not practical, in related or accompanying documentation.

ISL 2013-06 #3 (4-208). This paragraph provides detailed guidance for the derivative classifier. Unless otherwise evident, the “Classified By” Line shall include the company name and when applicable the division or branch, followed by the name and position or personal identifier of the derivative classifier.

Training: Contractor cleared personnel must be trained initially and at least once every 2 years on the topics set forth in NISPOM paragraph 4-102 before being authorized to make derivative classification decisions after December 31, 2013.

Contractor cleared personnel who can document that they have completed initial derivative classifier training required by NISPOM paragraph 4-102, do

not need to take additional derivative classifier training until 2 years have elapsed from the date of their initial training.

Contractors can develop and implement internal training programs or use an existing training course that includes, at a minimum, the topics set forth in NISPOM paragraph 4-102 to meet the NISPOM requirements of derivative classification training for contractor personnel who are authorized to make derivative classification decisions.

Contractors will retain records of the date of the most recent training (initial or refresher) and type of training derivative classifiers receive. Records of training must be available for review during DSS security vulnerability assessments. Records may consist of training attendance records, certificates, or other documentation verifying that personnel assigned duties as derivative classifiers have successfully completed the training requirements outlined in this ISL. If contractor employees perform derivative classification only at a customer location, they may receive training from either the contractor or the customer, but the contractor will maintain a copy of the record of training.

Training resources

The Derivative Classification Training Job Aid at the Center for Development of Security Excellence (CDSE) website has detailed guidance: <http://www.cdse.edu/documents/cdse/DerivativeClassification.pdf>.

Contractors who wish to use CDSE products can find their courseware on derivative classification at:

- <http://cdsetrain.dtic.mil/derivative/index.htm> (This course includes an exam built into the course. A STEPP account is not required for access to the course.)
- <http://www.cdse.edu/catalog/elearning/IF103.html>. (This course has a separate exam the cleared contractor must pass in order to receive credit for this course. A STEPP account is required for access to the course and exam.)

In addition to the above derivative classification training, the following marking course and training material provides additional information and

guidance on derivative classification marking requirements.

- CDSE - Marking Classified Information IF105.16
<http://www.cdse.edu/catalog/elearning/IF105.html>
- CDSE - Marking Classified Information (Job Aid)
https://stepp.dss.mil/courseware/markin/g_Classified_Information.pdf

a. **"CLASSIFIED BY" Line.** The purpose of the "Classified By" line is to identify the person who applies derivative classification markings for the document. If not otherwise evident, the line will include the agency and office of origin will be identified and follow the name and position or personal identifier of the derivative classifier.

b. **"DERIVED FROM" Line.** The purpose of the "Derived From" line is to link the derivative classification applied to the material by the contractor and the source document(s) or classification guide(s) under which it was classified. In completing the "Derived From" line, the contractor shall identify the applicable guidance that authorizes the classification of the material. Normally this will be a security classification guide listed on the Contract Security Classification Specification or a source document. When identifying a classification guide on the "Derived From" line, the guide's title or number, issuing agency, and date shall be included. Many Contract Security Classification Specifications cite more than one classification guide and/or the contractor is extracting information from more than one classified source document. In these cases, the contractor may use the phrase "multiple sources." When the phrase "multiple sources" is used, the contractor shall include a listing of the source materials in, or attached to, each derivatively classified document. This listing may take the form of a bibliography identifying the applicable classification sources.

c. **"DECLASSIFY ON" Line.** The purpose of the "Declassify On" line is to provide declassification instructions appropriate for the material. When completing this line, the contractor shall use the information specified in the Contract Security

Classification Specification or classification guide furnished with a classified contract. Or, the contractor shall carry forward the duration instruction from the source document or classification guide (e.g., date or event). When the source is marked "Original Agency's Determination Required" (OADR), "X1 through X8", Manual Review (MR), "DNI Only," "DCI Only," or contains any other no longer valid declassification instruction, the "Declassify On" line shall be marked with a date that is 25 years from the date of the source document, unless other guidance has been provided by the OCA. When a document is classified derivatively on the basis of more than one source document or more than one element of a classification guide, the "Declassify On" line shall reflect the longest duration of any of its sources. Material containing RD or FRD shall not have a "Declassify On" line unless co-mingled with national security information subject to reference (b).

d. **"DOWNGRADE TO" Line.** When downgrading instructions are contained in the Contract Security Classification Specification, classification guide or source document a "Downgrade To" line will be included. When completing this line, the contractor shall insert SECRET or CONFIDENTIAL and an effective date or event. The markings used to show this information are:

DERIVED FROM

DOWNGRADE TO ON

DECLASSIFY ON

e. **"REASON CLASSIFIED" Line.** As a general rule, a "Reason Classified" line will be shown only on originally classified documents. However, certain agencies may require that derivatively classified documents contain a "Reason Classified" Line to identify the specific reason for the derivative classification. Instructions for the use of these lines will be included in the security classification guidance provided with the contract.

4-209. Documents Generated Under Previous E.O.s. Documents classified under previous E.O.s need not be re-marked to comply with the marking requirements of reference (b).

a. Classified material originated under recent E.O.s contains overall, portion, paragraph, and appropriate downgrading and declassification markings that will provide sufficient guidance for the classification of extracted information. However, classified material originated under previous E.O.s may not have these markings. If the source document does not contain portion markings, the overall classification of the source document shall be used for the extracted information in the new document.

b. The classification markings for a source document are the responsibility of the originator and not the contractor extracting the information. Contractors are encouraged to contact the originator to avoid improper or unnecessary classification of material.

4-210. Marking Special Types of Material. The following procedures are for marking special types of material, but are not all inclusive. The intent of the markings is to ensure that the classification of the item, regardless of its form, is clear to the holder.

a. **Files, Folders, or Groups of Documents.** Files, folders, binders, envelopes, and other items containing classified documents, when not in secure storage, shall be conspicuously marked with the highest classification of any classified item included in the group. Cover sheets may be used for this purpose.

b. **E-mail and other Electronic Messages.** Electronically transmitted messages shall be marked in the same manner required for other documents except as noted. The overall classification of the message shall be the first item of information in the text and shall be displayed at the top and bottom of each message. A "Classified By" line, a "Derived From" line, a "Declassify On" line, and portion markings are required on messages. Certain agencies may also require that messages contain a "Reason Classified" line in order to identify the specific reason for classification, which is carried over from the source document(s) or classification guide. Instructions for the use of such lines will be included in the security classification guidance provided with the contract documents. E-mail transmitted on or prepared for transmission on classified systems or networks shall be configured to display:

(1) The overall classification at the top and bottom of the body of each message; the overall classification marking string for the e-mail will reflect the classification of the header and body of the message, including the subject line, the text of the e-mail, a classified signature block, attachments, included messages, and any other information conveyed in the body of the e-mail; classified e-mail will be portion marked.

(2) When forwarding or replying to an e-mail, contractors shall ensure that the classification markings reflect the overall classification and declassification instructions for the entire string of e-mails and attachments. This includes any newly drafted material, material received from previous senders, and any attachments.

(3) When messages are printed by an automated system, all markings may be applied by that system, provided the classification markings are clearly distinguished from the printed text. The markings required by paragraph 4-208 shall be included after the signature block, but before the overall classification marking at the end of the e-mail. The last line of the message shall be the overall classification of the e-mail.

c. **Microforms.** Microforms contain images or text in sizes too small to be read by the unaided eye. The applicable markings shall be conspicuously marked on the microform medium or its container to be readable by the unaided eye. These markings shall also be included on the image so that when the image is enlarged and displayed or printed, the markings will be conspicuous and readable. Further markings and handling shall be as appropriate for the particular microform involved.

d. **Translations.** Translations of U.S. classified information into a language other than English shall be marked to show the United States as the country of origin, with the appropriate U.S. markings and the foreign language equivalent.

4-211. Marking Transmittal Documents. A transmittal document shall be marked with the highest level of classified information contained in the document and with an appropriate notation to indicate its classification when the enclosures are removed. An unclassified document that transmits a

classified document as an attachment shall bear a notation substantially as follows: "Unclassified when Separated from Classified Enclosures." A classified transmittal that transmits higher classified information shall be marked with a notation substantially as follows: "CONFIDENTIAL (or SECRET) when Separated from Enclosures." In addition, a classified transmittal itself must bear all the classification markings required for a classified document.

4-212. Marking Wholly Unclassified Material. Normally, wholly UNCLASSIFIED material will not be marked or stamped UNCLASSIFIED unless it is essential to convey to a recipient of such material that (a) the material has been examined specifically with a view to impose a security classification and has been determined not to require classification; or (b) the material has been reviewed and has been determined to no longer require classification and it is declassified.

4-213. Marking Compilations. In some instances, certain information that would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. When classification is required to protect a compilation of such information, the overall classification assigned to the compilation shall be conspicuously affixed. The reason for classifying the compilation shall be stated at an appropriate location at or near the beginning of the compilation. Any unclassified portions will be portion marked (U), while the overall markings will reflect the classification of the compiled information, even if all the portions are marked (U).

4-214. Working Papers. Working papers containing classified information shall be dated when created; marked with the highest classification of any information contained in them; protected at that level; and if otherwise appropriate, destroyed when no longer needed. Working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level if released outside of the facility, filed permanently, or retained for more than 180 days from the date of the origin, filed permanently, e-mailed within or released outside the originating activity.

4-215. Marking Miscellaneous Material. Material developed in connection with the handling, processing, production, storage and utilization of classified information shall be handled in a manner that ensures adequate protection of the classified information involved and shall be destroyed at the earliest practical time, unless a requirement exists to retain such material. There is no requirement to mark such material.

4-216. Marking Training Material. Unclassified documents or materials that are created to simulate or demonstrate classified documents or material shall be clearly marked to indicate the actual UNCLASSIFIED status of the information. For example: SECRET FOR TRAINING PURPOSES ONLY, OTHERWISE UNCLASSIFIED or UNCLASSIFIED SAMPLE, or a similar marking may be used.

4-217. Downgrading or Declassification Actions. When documents or material that have been downgraded or declassified are removed from storage for use or for transmittal outside the facility, they shall be re-marked according to paragraph a or b below. If the volume of material is such that prompt re-marking of each classified item cannot be accomplished without unduly interfering with operations, a downgrading and declassification notice may be attached to the inside of the file drawers or other storage container instead of the re-marking otherwise required. Each notice shall specify the authority for the downgrading or declassification action, the date of the action, and the storage container to which it applies. When documents or other material subject to downgrading or declassification are withdrawn from the container solely for transfer to another, or when the container is transferred from one place to another, the transfer may be made without re-marking if the notice is attached to the new container or remains with each shipment.

a. Prior to taking any action to downgrade or declassify information, the contractor shall seek guidance from the GCA. If such action is approved, all old classification markings shall be canceled and the new markings substituted, whenever practical. In the case of documents, as a minimum the outside of the front cover, the title page, the first page, and the outside of the back shall reflect the new classification

markings, or the designation UNCLASSIFIED. Other material shall be re-marked by the most practical method for the type of material involved to ensure that it is clear to the holder what level of classification is assigned to the material.

ISL 2006-01 #8 (4-107 and 4-2167.a). Material Marked for Automatic Declassification. The term “automatic” declassification would seem to indicate that when classified material is marked with a declassification date, the contractor is authorized to automatically declassify the document. However, certain government agencies are concerned that, with all of the changes that have occurred to the declassification policy over the years, information may still retain sensitivity and therefore should not be “automatically” declassified.

When the contractor has material marked for automatic declassification, and notes that the date or event for the automatic declassification has occurred, the contractor must seek guidance from the government activity that released the information using the procedures of NISPOM paragraph 4-104. In effect, contractors are not authorized to unilaterally declassify even when the material is marked for automatic declassification.

b. When contractors are notified of downgrading or declassification actions that are contrary to the markings shown on the material, the material shall be re-marked to indicate the change. In addition, the material shall be marked to indicate the authority for the action, the date of the action, and the identity of the person or contractor taking the action. Other holders shall be notified if further dissemination has been made by the contractor.

4-218. Upgrading Action

ISL 2006-02 #5 (1-303 and 4-218). Notification to Recipients Regarding the Inadvertent Dissemination of Classified as Unclassified (ISL 00L-1 #8). Contractors are reminded that when classified information is transmitted or disseminated as unclassified, notification of the actual classification to recipients who are cleared for access to the material is, at a minimum, CONFIDENTIAL. Therefore, if the material was originally transmitted electronically, contractors must provide the classification notification via secure channels (e.g.,

cleared network, STU-III, secure fax). The notification should also provide the classification source as well as declassification instructions. When control of the material has been lost, or if unauthorized personnel have had access to the information, such as when the recipient is not cleared for access, the matter is to be reported to your DSS Field Office as a report of compromise. Regardless of whether the recipient is a cleared or uncleared contractor/individual, if the transmission occurred by an unsecure means, (i.e. unsecure fax, Internet, unclassified server, etc.), the control of the material is deemed lost.

a. When a notice is received to upgrade material to a higher level, for example from CONFIDENTIAL to SECRET, the new markings shall be immediately entered on the material according to the notice to upgrade, and all the superseded markings shall be obliterated. The authority for and the date of the upgrading action shall be entered on the material. Other holders shall be notified as appropriate if further dissemination of the material has been made by the contractor.

b. The contractor’s notice shall not be classified unless the notice contains additional information warranting classification. In the case of material which was inadvertently released as UNCLASSIFIED, the contractor’s notice shall be classified CONFIDENTIAL, unless it contains additional information warranting a higher classification. The notice shall cite the applicable Contract Security Classification Specification or other classification guide on the "Derived From" line and be marked with an appropriate declassification instruction.

4-219. Inadvertent Release. If classified material is inadvertently distributed outside the facility without the proper classification assigned to it, or without any markings to identify the material as classified, the contractor shall, as appropriate:

a. Determine whether all holders of the material are cleared and authorized access to it.

b. Determine whether control of the material has been lost.

c. If recipients are cleared for access to the material, promptly provide written notice to all holders of the proper classification to be assigned. If control of the material has been lost, if all copies cannot be accounted for, or if unauthorized personnel have had access to it, report the compromise to the CSA.

4-220. Marking requirements for transfers of defense articles to the United Kingdom. Marking requirements for transfers of defense articles to the

United Kingdom without a license or other written authorization are located in Chapter 10, Section 8 of this Manual.

4-221. Comingling of Restricted Data and Formerly Restricted Data. To the greatest degree possible, do not comingle RD and FRD in the same document with information classified pursuant to reference (b). When mixing can't be avoided, the requirements of references (b) and (z) must be met.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

CHAPTER 5

Safeguarding Classified Information

Section 1. General Safeguarding Requirements

5-100. General. Contractors shall be responsible for safeguarding classified information in their custody or under their control. Individuals are responsible for safeguarding classified information entrusted to them. The extent of protection afforded classified information shall be sufficient to reasonably foreclose the possibility of its loss or compromise.

5-101. Safeguarding Oral Discussions. Contractors shall ensure that all cleared personnel are aware of the prohibition against discussing classified information over unsecured telephones, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

5-102. End of Day Security Checks

a. Contractors that store classified material shall establish a system of security checks at the close of each working day to ensure that all classified material and security repositories have been appropriately secured.

b. Contractors that operate multiple work shifts shall perform the security checks at the end of the last working shift in which classified material was removed from storage for use. The checks are not required during continuous 24-hour operations.

5-103. Perimeter Controls. Contractors authorized to store classified material shall establish and maintain a system to deter and detect unauthorized introduction or removal of classified material from their facility. The objective is to discourage the introduction or removal of classified material without proper authority. If the unauthorized introduction or removal of classified material can be reasonably foreclosed through technical means, which are encouraged, no further controls are necessary.

Personnel who have a legitimate need to remove or transport classified material should be provided appropriate authorization for passing through designated entry/exit points. The fact that persons who enter or depart the facility are subject to an inspection of their personal effects shall be conspicuously posted at all pertinent entries and exits.

a. All persons who enter or exit the facility shall be subject to an inspection of their personal effects, except under circumstances where the possibility of access to classified material is remote. Inspections shall be limited to buildings or areas where classified work is being performed. Inspections are not required of wallets, change purses, clothing, cosmetics cases, or other objects of an unusually personal nature.

b. The extent, frequency, and location of inspections shall be accomplished in a manner consistent with contractual obligations and operational efficiency. Inspections may be done using any appropriate random sampling technique. Contractors are encouraged to seek legal advice during the formulation of implementing procedures and to surface significant problems to the CSA.

5-104. Emergency Procedures. Contractors shall develop procedures for safeguarding classified material in emergency situations. The procedures shall be as simple and practical as possible and should be adaptable to any type of emergency that may reasonably arise. Contractors shall promptly report to the CSA any emergency situation that renders the facility incapable of safeguarding classified material.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 2. Control and Accountability

5-200. Policy. Contractors shall establish an information management system to protect and control the classified information in their possession. Contractors shall ensure that classified information in their custody is used or retained only for a lawful and authorized U.S. Government purpose. The U.S. Government reserves the right to retrieve its classified material or to cause appropriate disposition of the material by the contractor. The information management system employed by the contractor shall be capable of facilitating such retrieval and disposition in a reasonable period of time.

ISL 2006-01 #9 (5-200). Information Management System. While the requirement to maintain external receipt and dispatch records for SECRET and CONFIDENTIAL information is eliminated, there is a requirement in the NISPOM for contractors to establish an information management system to protect and control the classified information in their possession. The purpose of this requirement is to ensure that contractors have the capability to retrieve classified material when necessary and to ensure the appropriate disposition of classified material in a reasonable period of time. There is no required format for such an information management system, no expectation that such a system must be in an electronic database, or that such a system incorporates any form of receipt and dispatch records. The contractor merely has to demonstrate capability for timely retrieval of classified information within the company and the capability to dispose of any and all classified information in its possession when required to do so.

5-201. Accountability for TOP SECRET

a. TOP SECRET control officials shall be designated to receive, transmit, and maintain access and accountability records for TOP SECRET information. An inventory shall be conducted annually unless written relief is granted by the GCA.

b. The transmittal of TOP SECRET information shall be covered by a continuous receipt system both within and outside the facility.

c. Each item of TOP SECRET material shall be numbered in series. The copy number shall be placed

on TOP SECRET documents and on all associated transaction documents.

5-202. Receiving Classified Material. Procedures shall be established to ensure that classified material, regardless of delivery method, is received directly by authorized personnel. The material shall be examined for evidence of tampering and the classified contents shall be checked against the receipt. Discrepancies in the contents of a package or absence of a receipt for TOP SECRET and SECRET material shall be reported promptly to the sender. If the shipment is in order, the receipt shall be signed and returned to the sender. If a receipt is included with CONFIDENTIAL material, it shall be signed and returned to the sender.

ISL 2006-01 #10 (5-202). Classified material coming into a facility, regardless of delivery method, must be received directly by authorized personnel. An authorized person means a cleared person who has been assigned this duty and therefore has need-to-know. The personnel who pick up the mail or accept deliveries from commercial delivery companies approved for transmitting classified material must be cleared to the level of classified material expected to be received by the contractor.

ISL 2006-01 #11 (5-202 and 5-401). Package Receipts and Receipt and Dispatch Records. The requirement to maintain external receipt and dispatch records for SECRET and CONFIDENTIAL information, regardless of the media of the information, has been eliminated.

While the requirement to maintain external receipt and dispatch records for SECRET and CONFIDENTIAL information has been eliminated, the requirement to include a receipt in the transmittal package for TOP SECRET and SECRET material remains. CONFIDENTIAL information does not require that a receipt be included in the transmittal package unless the sender deems it necessary. The receipt that is included in a transmittal package must be signed by the recipient and returned to the sender. The sender is required to maintain a suspense system to track transmitted material until a signed copy of the receipt is returned.

5-203. Generation of Classified Material

a. A record of TOP SECRET material produced by the contractor shall be made when the material is: (1) completed as a finished document, (2) retained for more than 180 days after creation, regardless of the stage of development, or (3) transmitted outside the facility.

b. Classified working papers generated by the contractor in the preparation of a finished document shall be: (1) dated when created, (2) marked with its overall classification and with the annotation "WORKING PAPERS", and (3) destroyed when no longer needed. Working papers shall be marked in the same manner prescribed for a finished document at the same classification level if released outside the facility, or retained for more than 180 days from the date of origin.

Section 3. Storage and Storage Equipment

5-300. General. This section describes the uniform requirements for the physical protection of classified material in the custody of contractors. Where these requirements are not appropriate for protecting specific types or forms of classified material, compensatory provisions shall be developed and approved by the CSA. Nothing in this manual shall be construed to contradict or inhibit compliance with the law or building codes. Cognizant security officials shall work to meet appropriate security needs according to the intent of this manual and at acceptable cost

5-301. GSA Storage Equipment. GSA establishes and publishes uniform standards, specifications, and supply schedules for units and key-operated and combination padlocks suitable for the storage and protection of classified information. Manufacturers and prices of storage equipment approved by the GSA are listed in the Federal Supply Schedule (P55) catalog (FSC GROUP 71-Pan II). Copies of specifications and schedules may be obtained from any regional office of the GSA.

ISL 2012-04 #1 (5-301). GSA-approved storage equipment, within the GSA Federal Supply Schedule, includes modular vaults, which can be used for the storage of classified information. The federal specifications and general requirements are set forth in FED-STD 832, "Construction Methods and Materials for Vaults," dated September 1, 2002. These specifications are equivalent to the criteria found in NISPOM paragraph 5-802, "Construction Required for Vaults."

For additional information, see:
<http://www.gsa.gov/portal/content/103856>.

5-302. TOP SECRET Storage. TOP SECRET material shall be stored in a GSA-approved security container, an approved vault, or an approved closed area with supplemental controls.

5-303. SECRET Storage. SECRET material shall be stored in a GSA-approved security container, an approved vault, or closed area. Supplemental controls are required for storage in closed areas. The following additional storage methods may be used until October 1, 2012:

ISL 2012-04 #2 (5-303). NISPOM paragraph 5-303 requires SECRET material to be stored in GSA-approved security containers, an approved vault, or closed area, and further prohibits storage using non-GSA approved security containers beginning on October 1, 2012. The Defense Security Service (DSS) places special emphasis on this requirement during recurring assessments. DSS will continue to review contractor plans to meet the deadline, which should include a timetable for identifying and eliminating all remaining non-GSA-approved containers being used to store classified material, and other actions being taken to prepare for this transition (e.g. transfer of classified holdings to other approved storage methods, disposing of classified information, or digitizing essential material). There is no requirement to retrofit locks on existing GSA approved security containers if the integrity of the container is intact and the GSA label is still affixed. When locks are determined to be unserviceable, the replacement lock must comply with Federal Specification FF-L-2740.

Additional information can be found on the DoD Lock Program website:
https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_wpp/navfac_nfesc_pp/locks

ISL 2014-03 #1 (5-301). In accordance with NISPOM paragraph 5-301, the procurement of new secure storage equipment must be in conformance with the standards and specifications established by the General Services Administration (GSA). The Information Security Oversight Office (ISOO) notices 2012-04 and 2014-02 provides additional guidance to the Federal government on the safeguarding of classified national security information in GSA approved security containers and addresses the procurement of these containers. Cleared contractors should be aware of the requirements outlined in the ISOO notice when purchasing GSA approved security containers.

The requirement to procure GSA-approved security containers from approved sources does not prevent the transfer or private sale of a GSA-approved security container originally obtained through a GSA-approved source by an end user.

A GSA approval label cannot be reproduced and can only be procured by Original Equipment Manufacturers (Qualified Product List Manufacturers) and by the GSA approved training institutions. Cleared contractors can verify replacement certification labels on their GSA-approved security containers by contacting the following two GSA-approved certifying schools who issue the recertification labels to persons authorized to inspect and recertify GSA-approved security containers and vault doors. Contact Lockmasters Security Institute for label serial numbers that begin with "LM" and MBA USA for label serial numbers that begin with "MBA."

Lockmasters Security Institute 1014 South Main Street Nicholasville, KY 40356 Phone: (800) 654-0637 Phone: (859) 885-6041	MBA USA, Inc. 200 Orchard Drive Nicholasville, KY 40356 Phone: (888) 622-5495 Phone: (859) 887-0496
--	---

Repair procedures for GSA approved containers and vault doors are outlined in [Federal Standard 809B, "Neutralization and Repair of GSA Approved Containers and Vault Doors."](#)

For any other questions, call the DoD Lock Program at 800-290-7607 or DSN: 551-1212.

a. A safe, steel file cabinet, or safe-type steel file container that has an automatic unit locking mechanism. All such receptacles will be accorded supplemental protection during non-working hours.

b. Any steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock. The keepers of the rigid metal lock bar shall be secured to the cabinet by welding, rivets, or bolts so they cannot be removed and replaced without leaving evidence of the entry. The drawers of the container shall be held securely so their contents cannot be removed without forcing open the drawer. This type of cabinet will be accorded supplemental protection during non-working hours.

5-304. CONFIDENTIAL Storage. CONFIDENTIAL material shall be stored in the same manner as TOP SECRET or SECRET material except that no supplemental protection is required.

5-305. Restricted Areas. When it is necessary to control access to classified material in an open area during working hours, a restricted area may be established. A restricted area will normally become necessary when it is impractical or impossible to protect classified material because of its size, quantity or other unusual characteristic. The restricted area shall have a clearly defined perimeter, but physical barriers are not required. Personnel within the area shall be responsible for challenging all persons who may lack appropriate access authority. All classified material will be secured during non-working hours in approved repositories or secured using other methods approved by the CSA.

5-306. Closed Areas. Due to the size and nature of the classified material, or for operational necessity, it may be necessary to construct closed areas for storage because GSA-approved containers or vaults are unsuitable or impractical. Closed areas must be constructed in accordance with section 8 of this chapter. Access to closed areas must be controlled to preclude unauthorized access. This may be accomplished through the use of a cleared person or by a supplanting access control device or system. Access shall be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified material/information within the area. Persons without the appropriate level of clearance and/or need to know shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented. Closed areas storing TOP SECRET and SECRET material shall be accorded supplemental protection during non-working hours. During non-working hours and during working hours when the area is unattended, admittance to the area shall be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. It is not necessary to activate the supplemental controls during working hours. Doors secured from the inside with a panic bolt (for example, actuated by a panic bar, a dead bolt, a rigid wood or metal bar) or other

means approved by the CSA, will not require additional locking devices.

ISL 2006-01 #12 (5-306). Securing Closed Areas. Closed areas storing TOP SECRET and SECRET material must have supplemental protection during non-working hours. During non-working hours and during working hours when the area is unattended, admittance to the area must be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. During working hours when the area is unattended, closed areas must be locked, but need not be alarmed.

The definition of working hours is that time during which the work force in the closed area is working on a regularly scheduled shift.

ISL 2006-01 #13 (5-306). Self-Approval Authority. Paragraph 5-306d of the NISPOM allows for the CSA to grant self-approval authority to qualified FSOs in establishing closed areas. The FSO may delegate this responsibility. Examples of qualifying criteria include successful experience following CSA procedures in establishing a closed area, completion of training which included classified material safeguarding and closed area requirements, and the facility security program having a CSA rating of satisfactory or better. If a cleared contractor facility wishes to nominate the FSO or designee to be authorized to approve closed areas, the facility should forward a request to the attention of the IS Rep responsible for the facility. The CSA will designate personnel granted this authority in writing.

ISL 2007-01, #1 (5-306, 8-100.b.). Must classified materials incidental to the operation of Information Systems (IS) maintained in the Closed Area be stored in GSA approved containers?

Answer: Classified material, which includes magnetic and electronic media as well as printed materials, are normally to be stored in approved security containers within the Closed Area during non-working hours or when the area is unattended unless the area has been approved for open shelf or bin storage in accordance with NISPOM paragraph 5-306b. Large items essential to the operation of an IS do not need to be secured in approved security containers in the Closed Area, provided all personnel

with access to the Closed Area have the clearance and need-to-know for all classified information within the Closed Area. Examples of items that do not need to be stored in security containers inside the Closed Area include large removable hard drives that are not easily disconnected from the IS or physically moved, or can be damaged by constant removal, or other media and technical manuals that need to be readily accessible for ongoing classified processing.

a. Contractors shall develop and implement procedures to ensure the structural integrity of closed areas above false ceilings and below raised floors.

ISL 2006-02 #15 (5-306.a.). Structural Integrity of Closed Areas (Reissue of ISL 03L-1 #4). When a Closed Area has a false ceiling and/or raised floor, the areas above the false ceiling and below the raised floor are part of the Closed Area. These areas are often not visible, and may provide opportunities for surreptitious entry, modifications or tampering. Contractors must develop and implement procedures to ensure the continued structural integrity of Closed Areas. One of the following options may be selected:

a) Alarming the area above the false ceiling and/or below the raised floor.

b) Establishing certain ceiling tiles or installing clear tiles to facilitate viewing around the periphery of the area so that the integrity of the walls above the false ceiling and below the raised floor can be verified during normal operations.

c) Establishing an internal procedure that all work orders involving closed areas must be approved by the FSO.

d) Periodically inspecting the areas above the false ceilings or below the raised floors by removing ceiling or floor tiles. Minimum intervals for inspecting the areas will vary depending on the nature of classified material stored in the Closed Area and overall security of the cleared contractor facility. The following matrix is provided as a guideline for determining an appropriate minimum inspection frequency. While this matrix provides a guide, in certain instances an accelerated or decelerated inspection frequency may be appropriate based on conditions at specific cleared facilities. The required minimum inspection frequency must be approved by

your Industrial Security Representative, and properly documented on the DSS Form 147, "Record of Controlled Areas."

ISL 2006-02 #15 Matrix (5-306.a.)

Nature of Classified Information	Security-in-Depth	Minimum Inspection Frequency
Classified Information Systems with unprotected transmission lines above false ceiling or below false floor	No	Monthly
	Yes	Every Six Months
Open Storage of Classified Documents	No	Monthly
	Yes	Every Six Months
Classified Hardware	No	Monthly
	Yes	Every Six Months

b. Open shelf or bin storage of SECRET and CONFIDENTIAL documents in closed areas requires CSA approval. For SECRET material only areas protected by an approved Intrusion Detection System (IDS) will qualify for such approval. Open shelf or bin storage of TOP SECRET documents is not permitted.

ISL 2012-04 #3 (5-306.b.). NISPOM paragraph 5-306b states that open shelf or bin storage (hereinafter referred to as "open storage") of SECRET and CONFIDENTIAL documents in closed areas requires Cognizant Security Agency approval. DSS will consider approving open storage of SECRET and CONFIDENTIAL material and information system (IS) media* in closed areas when the following additional conditions are met:

- The area is limited in size to that required to accommodate storage needs for classified material; or, the operational needs of the work performed in the area warrant open storage.
- The contractor ensures that visitors to such areas without the requisite personnel security clearance and need-to-know for all information stored in the area are denied access to the classified material contained therein.
- Entrance doors to the open storage area are secured by built-in GSA-approved electromechanical combination locks that meet Federal Specification FF-L-2740.
- For SECRET material, the area is protected by an approved intrusion detection system with a 30-minute response time, as well as security-in-

depth (SID) as determined by DSS. For open storage areas lacking sufficient SID, a 5-minute response time is required.

- For CONFIDENTIAL material, no supplemental protection or SID is required.
- The open storage area is within a facility, or specific portion of a facility, determined by DSS to have security-in-depth based on the following criteria:
 - The contractor has documented the specific layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility, or specified portion of the facility in which open storage is approved. During self-inspections, the contractor must review the effectiveness of these controls and report any changes affecting those controls to DSS.
 - At a minimum, the contractor has considered the following elements in their security-in-depth assessment:
 - Perimeter controls
 - Badge systems when the size of the population of the facility render personal recognition impracticable
 - Controlled access to sections of the facility in which classified work is performed
 - Access control devices when circumstances warrant

While existing DSS-approved open storage areas do not require re-approval, contractors must request DSS

approval for open storage if they want to use existing closed areas for this purpose. DSS will evaluate the closed area against the criteria provided above for approval.

(*Note: The presence of fixed media such as internal, non-removable hard drives in operational information systems is not considered open storage.)

c. The CSA and the contractor shall agree on the need to establish, and the extent of, closed areas prior to the award of the contract, when possible, or when the need for such areas becomes apparent during contract performance.

d. The CSA may grant self-approval authority to the FSO for closed area approvals provided the FSO meets specified qualification criteria as determined by the CSA.

5-307. Supplemental Protection

a. IDS as described in section 9 of this Chapter shall be used as supplemental protection.

b. Security guards approved as supplemental protection prior to January 1, 1995, may continue to be utilized. When guards are authorized, the schedule of patrol is 2 hours for TOP SECRET material and 4 hours for SECRET material.

c. GSA-approved security containers and approved vaults secured with a locking mechanism meeting Federal Specification FF-L-2740 do not require supplemental protection when the CSA has determined that the GSA-approved security container or approved vault is located in an area of the facility with security-in-depth.

5-308. Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas. Only a minimum number of authorized persons shall have knowledge of combinations to authorized storage containers. Containers shall bear no external markings indicating the level of classified material authorized for storage.

a. A record of the names of persons having knowledge of the combination shall be maintained.

b. Security containers, vaults, cabinets, and other authorized storage containers shall be kept locked

when not under the direct supervision of an authorized person entrusted with the contents.

c. The combination shall be safeguarded in accordance with the highest classification of the material authorized for storage in the container.

d. If a record is made of a combination, the record shall be marked with the highest classification of material authorized for storage in the container.

5-309. Changing Combinations. Combinations shall be changed by a person authorized access to the contents of the container, or by the FSO or his or her designee. Combinations shall be changed as follows:

a. The initial use of an approved container or lock for the protection of classified material.

b. The termination of employment of any person having knowledge of the combination, or when the clearance granted to any such person has been withdrawn, suspended, or revoked.

ISL 2006-02 #17 (5-309.b.). (ISL 89 L-2 Q&A). Combinations must be changed upon the termination of employment of any person having knowledge of those combinations. Having knowledge and having access are not the same thing. A locksmith has access to every combination but may not have knowledge of any combinations other than his or her own. It is not realistic to require a contractor to change hundreds of combinations when a locksmith leaves. The only combinations which require changing are those for which the locksmith had personal knowledge and the combination to the container(s) housing the master list or copies of combinations.

c. The compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended.

d. At other times when considered necessary by the FSO or CSA.

5-310. Supervision of Keys and Padlocks. Use of key-operated padlocks are subject to the following requirements: (i) a key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for protection of classified

material; (ii) a key and lock control register shall be maintained to identify keys for each lock and their current location and custody; (iii) keys and locks shall be audited each month; (iv) keys shall be inventoried with each change of custody; (v) keys shall not be removed from the premises; (vi) keys and spare locks shall be protected equivalent to the level of classified material involved; (vii) locks shall be changed or rotated at least annually and shall be replaced after loss or compromise of their operable keys; and (viii) making master keys is prohibited.

5-311. Repair of Approved Containers. Repairs, maintenance, or other actions that affect the physical integrity of a security container approved for storage of classified information shall be accomplished only by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance and repair of containers. Repair procedures may be obtained from the CSA.

ISL 2006-01 #14 (5-311). While the procedures for repairing approved security containers have been removed from the NISPOM, repair standards have not changed. Repairs, maintenance, or other actions that affect the physical integrity of a security container must still be accomplished by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance and repair of containers.

a. An approved security container is considered to have been restored to its original state of security integrity if all damaged or altered parts are replaced with manufacturer's replacement or identical cannibalized parts. A signed and dated certification for each repaired container, provided by the repairer, shall be on file setting forth the method of repair used.

b. A container repaired using other than approved methods may be used for storage of SECRET material with supplemental controls only until October 1, 2012.

5-312. Supplanting Access Control Systems or Devices. Automated access control systems and electronic, mechanical, or electromechanical devices which meet the criteria stated in paragraphs 5-313 and 5-314, below, may be used to supplant contractor-authorized personnel or guards to control

admittance to closed areas during working hours. Approval of the FSO is required before effecting the installation of a supplanting access control device to meet a requirement of this Manual.

5-313. Automated Access Control Systems. The automated access control system must be capable of identifying the individual entering the area and authenticating that person's authority to enter the area.

a. Manufacturers of automated access control equipment or devices must assure in writing that their system will meet the following standards before FSOs may favorably consider such systems for protection of classified information:

(1) Chances of an unauthorized individual gaining access through normal operation of the equipment are no more than one in ten thousand.

(2) Chances of an authorized individual being rejected for access through normal operation of the equipment are no more than one in one thousand.

b. Identification of individuals entering the area can be obtained by an identification (ID) badge or card, or by personal identity.

(1) The ID badge or card must 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.

(2) Personal identity verification identifies the individual requesting access by some unique personal characteristic, such as, (a) fingerprint, (b) hand geometry, (c) handwriting, (d) retina, or (e) voice recognition.

c. In conjunction with an ID badge or card or personal identity verification, a personal identification number (PIN) is required. The PIN must be separately entered into the system by each individual using a keypad device. The PIN shall consist of four or more digits, randomly selected with no known or logical association with the individual. The PIN must be changed when it is believed to have been subjected to compromise.

d. Authentication of the individual's authorization to enter the area must be accomplished within the system by comparing the inputs from the ID badge or card or the personal identity verification device and the keypad with an electronic database of individuals authorized into the area. A procedure must be established for removal of the individual's authorization to enter the area upon reassignment, transfer or termination, or when the individual's PCL is suspended or revoked.

e. Locations where access transactions are, or can be displayed, and where authorization data, card encoded data and personal identification or verification data is input, stored, displayed, or recorded must be protected.

f. Control panels, card readers, keypads, communication or interface devices located outside the entrance to a closed area shall have tamper-resistant enclosures, be securely fastened to a wall or other structure, be protected by a tamper alarm, or secured with an approved combination padlock. Control panels located within a closed area shall require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism. Where areas containing TOP SECRET information are involved, tamper alarm protection is mandatory.

g. Systems that utilize transmission lines to carry access authorization, personal identification, or verification data between devices/equipment located outside the closed area shall receive circuit protection equal to or greater than that specified as Grade A by Underwriters Laboratories (UL).

h. Access to records and information concerning encoded ID data and PINs shall be restricted to individuals cleared at the same level as the highest classified information contained within the specific area or areas in which ID data or PINs are utilized. Access to identification or authorization data, operating system software or any identifying data associated with the access control system shall be limited to the least number of personnel possible. Such data or software shall be kept secured when unattended.

i. Records reflecting active assignments of ID badges/cards, PINs, levels of access, and similar

system-related records shall be maintained. Records concerning personnel removed from the system shall be retained for 90 days.

j. Personnel entering or leaving an area shall be required to immediately secure the entrance or exit point. Authorized personnel who permit another individual entrance into the area are responsible for confirming the individual's PCL and need-to-know. During shift changes and emergency situations, if the door remains open, admittance shall be controlled by a contractor-authorized person or guard stationed to supervise the entrance to the area.

5-314. Electronic, Mechanical, or Electro-mechanical Devices. Provided the classified material within the closed area is no higher than SECRET, electronic, mechanical, or electro-mechanical devices that meet the criteria below may be used to supplant contractor authorized personnel or guards to control admittance to closed areas during working hours. Devices may be used that operate by either a push-button combination that activates the locking device or by a control card used in conjunction with a push-button combination, thereby excluding any system that operates solely by the use of a control card.

a. The electronic control panel containing the mechanism by which the combination is set may be located inside or outside the closed area. When located outside the closed area, the control panel shall be securely fastened or attached to the perimeter barrier of the area and secured by an approved combination padlock. If the control panel is located within the closed area, it shall require only a minimal degree of physical security designed to preclude unauthorized access to the mechanism.

b. The control panel shall be installed in a manner that precludes an unauthorized person in the immediate vicinity from observing the selection of the correct combination of the push buttons, or have a shielding device mounted.

c. The selection and setting of the combination shall be accomplished by an employee of the contractor who is authorized to enter the area. The combination shall be changed as specified in paragraph 5-309. The combination shall be classified and safeguarded in accordance with the classification

of the highest classified material within the closed area.

d. Electrical gear, wiring included, or mechanical links (cables, rods, etc.) shall be accessible only from inside the area, or shall be secured within a protective covering to preclude surreptitious manipulation of components.

e. Personnel entering or leaving the area shall be required to secure the entrance or exit point immediately. Authorized personnel who permit another individual entrance into the area are responsible for confirming the individual's PCL and need-to-know. During shift changes and emergency situations, if the door remains open, admittance shall be controlled by a contractor-authorized person or guard stationed to supervise the entrance to the area.

Section 4. Transmission

5-400. General. Classified material shall be transmitted outside the contractor's facility in a manner that prevents loss or unauthorized access.

5-401. Preparation and Receipting

ISL 2006-01 #11 (5-202 and 5-401). Package Receipts and Receipt and Dispatch Records. The requirement to maintain external receipt and dispatch records for SECRET and CONFIDENTIAL information, regardless of the media of the information, has been eliminated.

While the requirement to maintain external receipt and dispatch records for SECRET and CONFIDENTIAL information has been eliminated, the requirement to include a receipt in the transmittal package for TOP SECRET and SECRET material remains. CONFIDENTIAL information does not require that a receipt be included in the transmittal package unless the sender deems it necessary. The receipt that is included in a transmittal package must be signed by the recipient and returned to the sender. The sender is required to maintain a suspense system to track transmitted material until a signed copy of the receipt is returned.

a. Classified information to be transmitted outside of a facility shall be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that CONFIDENTIAL information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, the addressee and the document, but shall contain no classified information. It shall be signed by the recipient and returned to the sender.

b. A suspense system will be established to track transmitted documents until a signed copy of the receipt is returned.

c. When the material is of a size, weight, or nature that precludes the use of envelopes, the

materials used for packaging shall be of such strength and durability to ensure the necessary protection while the material is in transit.

5-402. TOP SECRET Transmission Outside a Facility. Written authorization of the GCA is required to transmit TOP SECRET information outside of the facility. TOP SECRET material may be transmitted by the following methods within and directly between the United States and its territorial areas.

a. The Defense Courier Service, if authorized by the GCA.

b. A designated courier or escort cleared for access to TOP SECRET information.

c. By electrical means over CSA-approved secured communications security circuits, provided such transmission conforms with this Manual, the telecommunications security provisions of the contract, or as otherwise authorized by the GCA.

5-403. SECRET Transmission Outside a Facility. SECRET material may be transmitted by one of the following methods within and directly between the United States and its territorial areas:

a. By the methods established for TOP SECRET.

b. U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail. NOTE: The "Waiver of Signature and Indemnity" block on the U.S. Postal Service Express Mail Label 11-B may not be executed and the use of external (street side) express mail collection boxes is prohibited.

c. A cleared commercial carrier.

d. A cleared commercial messenger service engaged in the intracity/local area delivery (same day delivery only) of classified material.

e. A commercial delivery company, approved by the CSA, that provides nation-wide, overnight service with computer tracking and reporting features. Such companies need not be security cleared.

ISL 2014-01 (5-403e and 5-404). General Services Administration (GSA) Carriers for Overnight Delivery of SECRET and CONFIDENTIAL Classified Information. ISL 2006-02 Article 18 is hereby cancelled and superseded by this ISL, which clarifies the application of National Industrial Security Program Operating Manual (NISPOM) paragraph 5-403e, "SECRET Transmission Outside of a Facility," and 5-404, "CONFIDENTIAL Transmission Outside of a Facility," when using Cognizant Security Agency (CSA) approved commercial delivery companies for the delivery of SECRET and CONFIDENTIAL material.

NISPOM 5-403e and 5-404 allow the use of CSA-approved commercial delivery companies for transmission of SECRET and CONFIDENTIAL material. Cleared contractors may use overnight express carriers approved by GSA for domestic express delivery services under Multiple Award Schedule 48. The list of approved overnight express carriers is available at the GSA website¹.

This ISL serves as notice that CSA approval to use GSA-listed commercial delivery companies is granted only in accordance with the following stipulations:

- Facility security officers (FSOs) must establish and document company procedures to ensure the proper protection of incoming and outgoing classified packages for each cleared facility intending to use GSA-listed commercial delivery companies for overnight service.
- FSOs may use such overnight express carriers for SECRET and CONFIDENTIAL shipments only after DSS formally approves the procedures.
- The following requirements must be included in company procedures.
 - Carrier personnel shall not be notified that the package contains classified material.
 - Material must be prepared for transmission as described in NISPOM paragraph 5-401, except that a carrier's mailing envelope may be used as the outer wrapper.

- The outer address label should contain only the office or position/title, e.g., the "Security Office" or the "Facility Security Officer," of the destination facility.
- Senders may not use a post office box as the destination address. Instead, a street delivery address approved for overnight shipments must be obtained using the Facility Verification Request (FVR) function of the Industrial Security Facilities Database (ISFD) for contractor locations or from the security office of a government activity. Identification of a contractor's address from FVR listing as an authorized overnight delivery address indicates Cognizant Security Office (CSO) approval of the receiving facility's ability to securely accept such packages.
- Senders may not execute a signature release authorization on the shipping label (i.e., to allow delivery of a shipment without obtaining the recipient's signature) under any circumstances.
- Both the sending and receiving contractors must establish an approved classified overnight street address for incorporation by DSS in the ISFD FVR function before such shipments may begin.
- All classified material and packages will be transferred directly to a representative of the commercial delivery company. Drop boxes are not permitted (regardless of location of the drop box; e.g., external street-side locations or a building lobby).
- Commercial delivery companies may be used for overnight transmission of SECRET and CONFIDENTIAL material within the continental United States, except for classified Communications Security (COMSEC), North Atlantic Treaty Organization (NATO), and foreign government information. Requirements for shipping COMSEC and unclassified Controlled Cryptographic Information are in the National Security Agency/Central Security Service Policy Manual 3-16, "Control of Communications Security (COMSEC) Material."

- As a general rule, commercial delivery packages may only be shipped Monday through Thursday to ensure they don't remain in the possession of the commercial delivery company over a weekend. However, the CSO may grant local approval to ship material on Fridays if the receiver has appropriate procedures in place to ensure a cleared person will sign for the package on Saturday and secure it in approved storage.
- The sender must verify the mailing address is correct and confirm an authorized person will be available to receive the delivery. The receiving contractor must have written procedures detailing how incoming overnight shipments will be received, transferred within the facility, and protected.
- Employees who handle incoming overnight shipments addressed to the "Security Office" or the "Facility Security Officer" must be cleared.

¹ <http://gsa.gov/portal/category/21197>

f. Other methods as directed in writing by the GCA.

5-404. CONFIDENTIAL Transmission Outside a Facility. CONFIDENTIAL material shall be transmitted by the methods established for SECRET material, except that a commercial carrier does not have to be cleared, or by U.S. Postal Service Certified Mail.

5-405. Transmission Outside the United States and Its Territorial Areas. Classified material may be transmitted to a U.S. Government activity outside the United States or a U.S. territory only under the provisions of a classified contract or with the written authorization of the GCA.

a. TOP SECRET material may be transmitted by the Defense Courier Service, Department of State Courier System, or a courier service authorized by the GCA.

b. SECRET and CONFIDENTIAL material may be transmitted by: (1) registered mail through U.S. Army, Navy, or Air Force postal facilities; (2) by an appropriately cleared contractor employee; (3) by a U.S. civil service employee or military person, who has been designated by the GCA; (4) by U.S. and

Canadian registered mail with registered mail receipt to and from Canada and via a U.S. or a Canadian government activity; or (5) as authorized by the GCA.

5-406. Addressing Classified Material. Mail or shipments containing classified material shall be addressed to the Commander or approved classified mailing address of a Federal activity or to a cleared contractor using the name and classified mailing address of the facility. An individual's name shall not appear on the outer cover. This does not prevent the use of office code letters, numbers, or phrases in an attention line to aid in internal routing.

a. When it is necessary to direct SECRET or CONFIDENTIAL material to the attention of a particular individual, other than as prescribed below, the identity of the intended recipient shall be indicated on an attention line placed in the letter of transmittal or on the inner container or wrapper.

b. When addressing SECRET or CONFIDENTIAL material to an individual operating as an independent consultant, or to any facility at which only one employee is assigned, the outer container shall specify: "TO BE OPENED BY ADDRESSEE ONLY" and be annotated: "POSTMASTER-DO NOT FORWARD. IF UNDELIVERABLE TO ADDRESSEE, RETURN TO SENDER."

5-407. Transmission Within a Facility. Classified material may be transmitted within a facility without single or double-wrapping provided adequate measures are taken to protect the material against unauthorized disclosure.

5-408. SECRET Transmission by Commercial Carrier. SECRET material may be shipped by a cleared commercial carrier that has been approved by the CSA to transport SECRET shipments. Commercial carriers may be used only within and between the 48 contiguous States and the District of Columbia or wholly within Alaska, Hawaii, or a U.S. territory. When the services of a commercial carrier are required, the contractor, as consignor, shall be responsible for the following:

a. The material shall be prepared for transmission to afford additional protection against pilferage, theft, and compromise as follows.

(1) The material shall be shipped in hardened containers unless specifically authorized otherwise by the contracting agency.

(2) Carrier equipment shall be sealed by the contractor or a representative of the carrier when there is a full carload, a full truckload, exclusive use of the vehicle, or when a closed and locked compartment of the carrier's equipment is used. The seals shall be numbered and the numbers indicated on all copies of the bill of lading (BL). When seals are used, the BL shall be annotated substantially as follows: DO NOT BREAK SEALS EXCEPT IN CASE OF EMERGENCY OR UPON PRIOR AUTHORITY OF THE CONSIGNOR OR CONSIGNEE. IF FOUND BROKEN OR IF BROKEN FOR EMERGENCY REASONS, APPLY CARRIER'S SEALS AS SOON AS POSSIBLE AND IMMEDIATELY NOTIFY BOTH THE CONSIGNOR AND THE CONSIGNEE.

(3) For DoD contractors the notation "Protective Security Service Required" shall be reflected on all copies of the BL. The BL will be maintained in a suspense file to follow-up on overdue or delayed shipments.

b. The contractor shall utilize a qualified carrier selected by the U.S. Government that will provide a single-line service from point of origin to destination, when such service is available, or by such transshipping procedures as may be specified by the U.S. Government.

c. The contractor shall request routing instructions, including designation of a qualified carrier, from the GCA or designated representative (normally the government transportation officer). The request shall specify that the routing instructions are required for the shipment of SECRET material and include the point of origin and point of destination.

d. The contractor shall notify the consignee (including U.S. Government transshipping activity) of the nature of the shipment, the means of the shipment, numbers of the seals, if used, and the anticipated time and date of arrival by separate

communication at least 24 hours in advance (or immediately on dispatch if transit time is less than 24 hours) of the arrival of the shipment. This notification shall be addressed to the appropriate organizational entity and not to an individual. Request that the consignee activity (including a military transshipping activity) notify the consignor of any shipment not received within 48 hours after the estimated time of arrival indicated by the consignor.

e. In addition, the contractor shall annotate the BL: "CARRIER TO NOTIFY THE CONSIGNOR AND CONSIGNEE (Telephone Numbers) IMMEDIATELY IF SHIPMENT IS DELAYED BECAUSE OF AN ACCIDENT OR INCIDENT. IF NEITHER CAN BE REACHED, CONTACT (Enter appropriate HOTLINE Number). USE HOTLINE NUMBER TO OBTAIN SAFE HAVEN OR REFUGE INSTRUCTIONS IN THE EVENT OF A CIVIL DISORDER, NATURAL DISASTER, CARRIER STRIKE OR OTHER EMERGENCY."

5-409. CONFIDENTIAL Transmission by Commercial Carrier. CONFIDENTIAL material may be shipped by a CSA or GCA-approved commercial carrier. For DoD contractors a commercial carrier authorized by law, regulatory body, or regulation to provide the required transportation service shall be used when a determination has been made by the Surface Deployment and Distribution Command (SDDC) (formerly known as the Military Traffic Management Command) that the carrier has a tariff, government tender, agreement, or contract that provides Constant Surveillance Service. Commercial carriers may be used only within and between the 48 contiguous states and the District of Columbia or wholly within Alaska, Hawaii, or a U.S. territory. An FCL is not required for the commercial carrier. The contractor, as consignor, shall:

a. Utilize containers of such strength and durability as to provide security protection to prevent items from breaking out of the container and to facilitate the detection of any tampering with the container while in transit;

b. For DoD contractors indicate on the BL, "Constant Surveillance Service Required." In addition, annotate the BL as indicated in 5-408e.

c. Instruct the carrier to ship packages weighing less than 200 pounds gross in a closed vehicle or a closed portion of the carrier's equipment.

5-410. Use of Couriers, Handcarriers, and Escorts. Contractors who designate cleared employees as couriers, handcarriers, and escorts shall ensure:

a. They are briefed on their responsibility to safeguard classified information.

b. They possess an identification card or badge which contains the contractor's name and the name and a photograph of the employee.

c. The employee retains classified material in his or her personal possession at all times. Arrangements shall be made in advance of departure for overnight storage at a U.S. Government installation or at a cleared contractor's facility that has appropriate storage capability, if needed.

d. If the classified material is being handcarried to a classified meeting or on a visit, an inventory of the material shall be made prior to departure. A copy of the inventory shall be carried by the employee. On the employee's return to the facility, an inventory shall be made of the material for which the employee was charged.

5-411. Use of Commercial Passenger Aircraft for Transmitting Classified Material. Classified material may be handcarried aboard commercial passenger aircraft by cleared employees with the approval of the FSO.

a. **Routine Processing.** Employees handcarrying classified material will be subject to routine processing by airline security agents. Hand-held packages will normally be screened by x-ray examination. If security personnel are not satisfied with the results of the inspection, and the prospective passenger is requested to open a classified package for visual examination the traveler shall inform the screener that the carry-on items contain U.S. Government classified information and cannot be opened. Under no circumstances may the classified material be opened by the traveler or security personnel.

b. **Special Processing.** When routine processing would subject the classified material to compromise

or damage; when visual examination is or may be required to successfully screen a classified package; or when classified material is in specialized containers which due to its size, weight, or other physical characteristics cannot be routinely processed, the contractor shall contact the appropriate air carrier in advance to explain the particular circumstances and obtain instructions on the special screening procedures to be followed.

c. **Authorization Letter.** Contractors shall provide employees with written authorization to handcarry classified material on commercial aircraft. The written authorization shall:

(1) Provide the full name, date of birth, height, weight, and signature of the traveler and state that he or she is authorized to transmit classified material;

(2) Describe the type of identification the traveler will present on request;

(3) Describe the material being handcarried and request that it be exempt from opening;

(4) Identify the points of departure, destination, and known transfer points;

(5) Include the name, telephone number, and signature of the FSO, and the location and telephone number of the CSA.

5-412. Use of Escorts for Classified Shipments. If an escort is necessary to ensure the protection of the classified information being transported, a sufficient number of escorts shall be assigned to each classified shipment to ensure continuous surveillance and control over the shipment while in transit. Specific written instructions and operating procedures shall be furnished escorts prior to shipping and shall include the following:

ISL 2006-01 #15 (5-412 and 10-402). The requirement for escorts for classified shipments applies only when an escort is determined to be necessary to ensure the protection of classified information during transport.

NISPOM paragraph 10-402 discusses transportation plans and the conditions under which international

carriers (e.g., commercial airlines) may be used to transport classified material internationally. The requirement for an escort is a matter to be determined by the U.S. approving authority for the transportation plan in consultation with the foreign government counterpart. Therefore, depending on specific circumstances and the judgment of the U.S. and foreign government approvers of the transportation plan, cleared escorts may or may not be required for international transfers.

a. Name and address of persons, including alternates, to whom the classified material is to be delivered;

b. Receipting procedures;

c. Means of transportation and the route to be used;

d. Duties of each escort during movement, during stops en route, and during loading and unloading operations; and

e. Emergency and communication procedures.

5-413. Functions of an Escort. Escorts shall be responsible for the following.

a. Accept custody for the shipment by signing a receipt and release custody of the shipment to the consignee after obtaining a signed receipt.

b. When accompanying a classified shipment in an express or freight car, provide continuous observation of the containers and observe adjacent areas during stops or layovers.

c. When traveling in an escort car accompanying a classified shipment via rail, keep the shipment cars

under observation and detrain at stops, when practical and time permits, in order to guard the shipment cars and check the cars or containers locks and seals. The escort car (after arrangements with the railroad) should be pre-positioned immediately behind the car used for the classified shipment to enable the escort to keep the shipment car under observation.

d. Maintain liaison with train crews, other railroad personnel, special police, and law enforcement agencies, as necessary.

e. When escorting classified shipments via motor vehicles, maintain continuous vigilance for the presence of conditions or situations that might threaten the security of the cargo, take such action as circumstances might require to avoid interference with continuous safe passage of the vehicle, check seals and locks at each stop where time permits, and observe vehicles and adjacent areas during stops or layovers.

f. When escorting shipments via aircraft, provide continuous observation of plane and cargo during ground stops and of cargo during loading and unloading operations. The escort shall not board the plane until after the cargo area is secured. Furthermore, the escort should preferably be the first person to depart the plane to observe the opening of the cargo area. Advance arrangements with the airline are required.

g. Notify the consignor by the fastest means available if there is an unforeseen delay en route, an alternate route is used, or an emergency occurs. If appropriate and the security of the shipment is involved, notify the nearest law enforcement official.

Section 5. Disclosure

5-500. General. Contractors shall ensure that classified information is disclosed only to authorized persons.

5-501. Disclosure to Employees. Contractors are authorized to disclose classified information to their cleared employees as necessary for the performance of tasks or services essential to the fulfillment of a classified contract or subcontract.

5-502. Disclosure to Subcontractors. Contractors are authorized to disclose classified information to a cleared subcontractor when access is necessary for the performance of tasks or services essential to the fulfillment of a prime contract or a subcontract.

5-503. Disclosure between Parent and Subsidiaries. Disclosure of classified information between a parent and its subsidiaries, or between subsidiaries, shall be accomplished in the same manner as prescribed in 5-502 for subcontractors.

ISL 2011-03 (5-503). Disclosure of Classified Information between Parent and Subsidiaries within a Corporate Family (NISPOM 5-503). NISPOM paragraph 5-503 requires that disclosure of classified information between a parent and its subsidiaries be accomplished in the same manner as disclosure between a prime contractor and a subcontractor. That means a classified subcontract must be in place between the legal entities involved to allow for such disclosures.

A valid facility clearance (FCL) at the same level, or higher, than the classified information to be disclosed must be in place between the legal entities involved to allow for such disclosures. The recipient of the information must also have a need-to-know (see NISPOM Appendix C definition) for the information involved and approved storage capability, if a physical transfer of classified material occurs.

The NISPOM definition of a subcontract includes purchase orders, service agreements, and other types of agreements or procurement actions between contractors that requires or will require access to classified information to fulfill the performance requirements of a prime contract. The agreement or procurement action that constitutes the subcontract

should be in writing and available for review by DSS. This clarification also applies to disclosure of classified information between any of the separate legal entities within the corporate family. The disclosure or transfer of the information must be in furtherance of a bona fide Government purpose.

Appropriate classification guidance for the classified information to be disclosed must be conveyed with the agreement or procurement action in the form of a Contract Security Classification Specification (DD Form 254), a security classification guide provided by the Government Contracting Activity (GCA), or other written security classification guidance.

All current waivers to the requirements of NISPOM paragraph 5-503 granted by DSS are no longer necessary, and are hereby cancelled.

5-504. Disclosure in an MFO. Disclosure of classified information between cleared facilities of the MFO shall be accomplished in the same manner as prescribed in 5-501 for employees.

5-505. Disclosure to DoD Activities. Contractors are authorized to disclose classified information received or generated under a DoD classified contract to another DoD activity unless specifically prohibited by the DoD activity that has classification jurisdiction over the information.

5-506. Disclosure to Federal Agencies. Contractors shall not disclose classified information received or generated under a contract from one agency to any other Federal agency unless specifically authorized by the agency that has classification jurisdiction over the information.

5-507. Disclosure of Classified Information to Foreign Persons. Contractors shall not disclose classified information to foreign persons unless release of the information is authorized in writing by the Government Agency having classification jurisdiction over the information involved, e.g. the DOE for RD and FRD, the NSA for COMSEC, the DNI for SCI, and all other Executive Branch departments and agencies for classified information under their jurisdiction. The disclosure must also be consistent with applicable U.S. laws and regulations.

5-508. Disclosure of Export Controlled Information to Foreign Persons. Contractors shall not disclose export-controlled information and technology (classified or unclassified) to a foreign person, whether an employee or not, or whether disclosure occurs in the United States or abroad, unless such disclosure is in compliance with applicable U.S. laws and regulations.

5-509. Disclosure to Other Contractors. Contractors shall not disclose classified information to another contractor except in furtherance of a contract, subcontract, or other GCA purpose.

5-510. Disclosure of Classified Information in Connection with Litigation. Contractors shall not disclose classified information to attorneys hired solely to represent the contractor in any civil or criminal case in Federal or state courts unless the disclosure is specifically authorized by the agency that has jurisdiction over the information. Contractors shall not disclose classified information to any Federal or state court except on specific instructions of the agency which has jurisdiction over the information or the attorney representing the United States in the case. (For criminal cases in Federal courts, see paragraph 1-208.)

5-511. Disclosure to the Public. Contractors shall not disclose classified or unclassified information pertaining to a classified contract to the public without prior review and clearance as specified in the Contract Security Classification Specification for the contract or as otherwise specified by the GCA.

a. Requests for approval shall be submitted through the activity specified in the GCA-provided classification guidance for the contract involved. Each request shall indicate the approximate date the contractor intends to release the information for public disclosure and identify the media to be used for the initial release. A copy of each approved request for release shall be retained for a period of one inspection cycle for review by the CSA. All

information developed subsequent to the initial approval shall also be cleared by the appropriate office prior to public disclosure.

b. The following information need not be submitted for approval unless specifically prohibited by the GCA:

(1) The fact that a contract has been received, including the subject matter of the contract and/or type of item in general terms provided the name or description of the subject matter is not classified.

(2) The method or type of contract; such as, bid, negotiated, or letter.

(3) Total dollar amount of the contract unless that information equates to (a) a level of effort in a sensitive research area, or (b) quantities of stocks of certain weapons and equipment that are classified.

(4) Whether the contract will require the hiring or termination of employees.

(5) Other information that from time-to-time may be authorized on a case-by-case basis in a specific agreement with the contractor.

(6) Information previously officially approved for public disclosure.

c. The procedures of this paragraph also apply to information pertaining to classified contracts intended for use in unclassified brochures, promotional sales literature, reports to stockholders, or similar material.

d. Information that has been declassified is not automatically authorized for public disclosure. Contractors shall request approval for public disclosure of "declassified" information in accordance with the procedures of this paragraph.

Section 6. Reproduction

5-600. General. Contractors shall establish a control system to ensure that reproduction of classified material is held to the minimum consistent with contractual and operational requirements. Classified reproduction shall be accomplished by authorized personnel knowledgeable of the procedures. The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified documents is encouraged.

5-601. Limitations

a. TOP SECRET documents may be reproduced as necessary in the preparation of a contract deliverable. Reproduction for any other purpose requires the consent of the GCA.

b. Unless restricted by the GCA, SECRET and CONFIDENTIAL documents may be reproduced as follows:

(1) Performance of a prime contract or a subcontract in furtherance of a prime contract.

(2) Preparation of a solicited or unsolicited bid, quotation, or proposal to a Federal agency or prospective subcontractor.

(3) Preparation of patent applications to be filed in the U.S. Patent Office.

c. Reproduced copies of classified documents shall be subject to the same protection as the original documents.

5-602. Marking Reproductions. All reproductions of classified material shall be conspicuously marked with the same classification markings as the material being reproduced. Copies of classified material shall be reviewed after the reproduction process to ensure that these markings are visible.

5-603. Records. Contractors shall maintain a record of the reproduction of all TOP SECRET material for 2 years.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 7. Disposition and Retention

5-700. General

a. Classified information no longer needed shall be processed for appropriate disposition. Classified information approved for destruction shall be destroyed in accordance with this section. The method of destruction must preclude recognition or reconstruction of the classified information or material.

b. Contractors shall establish procedures for review of their classified holdings on a recurring basis to reduce these classified inventories to the minimum necessary for effective and efficient operations. Multiple copies, obsolete material, and classified waste shall be destroyed as soon as practical after it has served its purpose. Any appropriate downgrading and declassification actions shall be taken on a timely basis to reduce the volume and to lower the level of classified material being retained by the contractor.

5-701. Retention of Classified Material. Contractors are authorized to retain classified material received or generated under a contract for a period of 2 years after completion of the contract, provided the GCA does not advise to the contrary. If retention is required beyond the 2-year period, the contractor must request and receive written retention authority from the GCA.

a. Contractors shall identify classified material for retention beyond 2 years as follows:

(1) TOP SECRET material shall be identified in a list of specific documents unless the GCA authorizes identification by subject matter and approximate number of documents.

(2) SECRET and CONFIDENTIAL material may be identified by general subject matter and the approximate number of documents.

b. Contractors shall include a statement of justification for retention based on the following:

(1) The material is necessary for the maintenance of the contractor's essential records.

(2) The material is patentable or proprietary data to which the contractor has title.

(3) The material will assist the contractor in independent research and development efforts.

(4) The material will benefit the U.S. Government in the performance of other prospective or existing agency contracts.

(5) The material will benefit the U.S. Government in the performance of another active contract and will be transferred to that contract (specify contract).

c. If retention beyond 2 years is not authorized, all classified material received or generated in the performance of a classified contract shall be destroyed unless it has been declassified or the GCA has requested that the material be returned.

5-702. Termination of Security Agreement. Notwithstanding the provisions for retention outlined above, in the event that the FCL is to be terminated, the contractor shall return all classified material in its possession to the GCA concerned, or dispose of such material in accordance with instructions from the CSA.

5-703. Disposition of Classified Material Not Received Under a Specific Contract.

a. Contractors shall return or destroy classified material received with a bid, proposal, or quote in accordance with the following schedule:

(1) If a bid, proposal, or quote is not submitted or is withdrawn within 180 days after the opening date of bids, proposals, or quotes.

(2) If a bid, proposal, or quote is not accepted within 180 days after notification that a bid, proposal, or quote has not been accepted.

b. If the classified material was not received under a specific contract, such as material obtained at classified meetings or from a secondary distribution center, within 1 year after receipt.

5-704. Destruction. Contractors shall destroy classified material in their possession as soon as possible after it has served the purpose for which it was released by the government, developed or prepared by the contractor, or retained after completion or termination of the contract.

ISL 2007-01 #54 (5-704, 5-705, 8-103.f., 8-301). Can DSS provide guidance on the clearing and sanitization requirements for classified material no longer required?

Answer. Yes, DSS has published the following updated DSS Clearing and Sanitization Matrix on the DSS web site (www.dss.mil) under the Industrial Security Program tab. (See Paragraph 8-301 for ISL matrix.)

5-705. Methods of Destruction. Classified material may be destroyed by burning, shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing (for example, hammer mills, choppers, and hybridized disintegration equipment). Pulpers, pulverizers, or shredders may be used only for the destruction of paper products. High wet strength paper, paper mylar, durable-medium paper substitute, or similar water repellent papers are not sufficiently destroyed by pulping; other methods such as disintegration, shredding, or burning shall be used to destroy these types of papers. Residue shall be inspected during each destruction to ensure that classified information cannot be reconstructed. Crosscut shredders currently in use capable of maintaining a shred size not exceeding 1/32 inch in width (with a 1/64 inch tolerance by 1/2 inch in length) may continue to be used. However, any crosscut shredders requiring replacement of the unit and/or rebuilding of the shredder blades assembly must be replaced by a crosscut shredder on the latest NSA Evaluated Products List of High Security Crosscut Shredders. The list may be obtained from the CSA. Classified material in microform; that is,

microfilm, microfiche, or similar high data density material; may be destroyed by burning or chemical decomposition, or other methods as approved by the CSA.

a. Public destruction facilities may be used only with the approval of, and under conditions prescribed by, the CSA.

b. Classified material removed from a cleared facility for destruction shall be destroyed on the same day it is removed.

5-706. Witness to Destruction. Classified material shall be destroyed by authorized personnel who have a full understanding of their responsibilities. For destruction of TOP SECRET material, two persons are required. For destruction of SECRET and CONFIDENTIAL material, one person is required.

5-707. Destruction Records. Destruction records are required for TOP SECRET material. The records shall indicate the date of destruction, identify the material destroyed, and be signed by the individuals designated to destroy and witness the destruction. Destruction officials shall be required to know, through their personal knowledge, that such material was destroyed. At the contractor's discretion, the destruction information required may be combined with other required control records. Destruction records shall be maintained by the contractor for 2 years.

5-708. Classified Waste. Classified waste shall be destroyed as soon as practical. This applies to all waste material containing classified information. Pending destruction, classified waste shall be safeguarded as required for the level of classified material involved. Receptacles utilized to accumulate classified waste shall be clearly identified as containing classified material.

Section 8. Construction Requirements

5-800. General. This section describes the construction requirements for closed areas and vaults. Construction shall conform to the requirements of this section or, with CSA approval, to the standards of Intelligence Community Directive 705, "Sensitive Compartmented Information Facilities (SCIFs) (reference (n)).

5-801. Construction Requirements for Closed Areas. This paragraph specifies the minimum safeguards and standards required for the construction of closed areas that are approved for use for safeguarding classified material. These criteria and standards apply to all new construction and reconstruction, alterations, modifications, and repairs of existing areas. They will also be used for evaluating the adequacy of existing areas.

a. **Hardware.** Only heavy-gauge hardware shall be used in construction. Hardware accessible from outside the area shall be peened, pinned, brazed, or spot welded to preclude removal.

b. **Walls.** Construction may be of material offering resistance to, and evidence of, unauthorized entry into the area. If insert-type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering. If visual access is a factor, area barrier walls up to a height of 8 feet shall be of opaque or translucent construction.

c. **Windows.** Windows that can be opened and that are less than 18 feet from an access point (for example, another window outside the area, roof, ledge, or door) shall be fitted with 1/2-inch bars (separated by no more than 6 inches), plus crossbars to prevent spreading, 18-gauge expanded metal or wire mesh securely fastened on the inside. When visual access of classified information is a factor, the windows shall be covered by any practical method, such as drapes, blinds, or paint covering the inside of the glass. During nonworking hours, the windows shall be closed and securely fastened to preclude surreptitious entry.

d. **Doors.** Doors shall be constructed of material offering resistance to and detection of unauthorized entry. When windows, louvers, baffle plates, or

similar openings are used, they shall be secured with 18-gauge expanded metal or with wire mesh securely fastened on the inside. If visual access is a factor, the windows shall be covered. When doors are used in pairs, an astragal (overlapping molding) shall be installed where the doors meet.

e. **Door Locking Devices.** Entrance doors shall be secured with either an approved built-in combination lock, an approved combination padlock, or with an approved key-operated padlock. Other doors shall be secured from the inside with a panic bolt (for example, actuated by a panic bar); a dead bolt; a rigid wood or metal bar (which shall preclude "springing") which extends across the width of the door and is held in position by solid clamps, preferably on the door casing; or by other means approved by the CSA consistent with relevant fire and safety codes.

f. **Ceilings.** Ceilings shall be constructed of material offering resistance to and detection of unauthorized entry. Wire mesh or other non-opaque material offering similar resistance to, and evidence of, unauthorized entry into the area may be used if visual access to classified material is not a factor.

g. **Ceilings (Unusual Cases).** When wall barriers do not extend to the true ceiling and a false ceiling is created, the false ceiling must be reinforced with wire mesh or 18-gauge expanded metal to serve as the true ceiling. When wire mesh or expanded metal is used, it must overlap the adjoining walls and be secured in a manner that precludes removal without leaving evidence of tampering. When wall barriers of an area do extend to the true ceiling and a false ceiling is added, there is no necessity for reinforcing the false ceiling. When there is a valid justification for not erecting a solid ceiling as part of the area, such as the use of overhead cranes for the movement of bulky equipment within the area, the contractor shall ensure that surreptitious entry cannot be obtained by entering the area over the top of the barrier walls.

h. **Miscellaneous Openings.** All vents, ducts and similar openings into closed areas that measure in excess of 96 square inches and over 6 inches in their smallest dimension must be protected with

either ½-inch diameter steel bars with a maximum space of 6 inches between the bars; grills consisting of 18-gauge expanded metal, wire mesh; or an equivalent gauge commercial metal duct barrier. The barriers must be secured to preclude removal from outside the area, and the method of installation must ensure that classified material cannot be removed through the openings with the aid of any type of instrument. A barrier will not be required if an approved IDS provides protection of the opening.

5-802. Construction Required for Vaults. This paragraph specifies the minimum standards required for the construction of vaults approved for use as storage facilities for classified material. These standards apply to all new construction and reconstruction, alterations, modifications, and repairs of existing vaults. They will also be used for evaluating the adequacy of existing vaults. In addition to the requirements given below, the wall, floor, and roof construction shall be in accordance with nationally recognized standards of structural practice. For the vaults described below, the concrete shall be poured in place and will have a compressive strength of 2,500 pounds per square inch.

a. **Floor.** The floor must be a monolithic concrete construction of the thickness of adjacent concrete floor construction, but not less than 4 inches thick.

b. **Walls.** Walls must be not less than 8-inch-thick hollow clay tile (vertical cell double shells) or concrete blocks (thick shells). Monolithic steel-reinforced concrete walls at least 4 inches thick may also be used. Where hollow clay tiles are used and such masonry units are flush, or in contact with, facility exterior walls, they shall be filled with concrete and steel-reinforced bars. Walls are to extend to the underside of the roof or ceiling above.

c. **Roof/Ceiling.** The roof or ceiling must be a monolithic reinforced concrete slab of a thickness to be determined by structural requirements.

d. **Vault Door and Frame Unit.** A GSA-approved vault door and frame unit shall be used.

e. **Miscellaneous Openings.** Omission of all miscellaneous openings is desirable, but not mandatory. Openings of such size and shape as to permit unauthorized entry, (normally in excess of 96 square inches in area and over 6 inches in its smallest dimension) and openings for ducts, pipes, registers, sewers and tunnels shall be equipped with man-safe barriers such as wire mesh, 18-gauge expanded metal, or rigid metal bars of at least 1/2 inch in diameter extending across their width with a maximum space of 6 inches between the bars. The rigid metal bars shall be securely fastened at both ends to preclude removal and, if the bars exceed 18 inches in length, shall have crossbars to prevent spreading. Where wire mesh, expanded metal, or rigid metal bars are used, care shall be exercised to ensure that classified material within the vault cannot be removed with the aid of any type of instrument. Pipes and conduits entering the vault shall enter through walls that are not common to the vault and the structure housing the vault. Preferably such pipes and conduits should be installed when the vault is constructed. If this is not practical, they shall be carried through snug-fitting pipe sleeves cast in the concrete. After installation, the annular space between the sleeve and the pipe or conduit shall be caulked solid with lead, wood, waterproof (silicone) caulking, or similar material, which will give evidence of surreptitious removal.

Section 9. Intrusion Detection Systems

5-900. General. This section specifies the minimum standards for an approved IDS when supplemental protection is required for TOP SECRET and SECRET material. The IDS shall be connected to, and monitored by, a central monitoring station. Alarm system installation shall conform to the requirements of this section or to the standards set forth in reference (n). The CSA will approve contingency protection procedures in the event of IDS malfunction.

5-901. CSA Approval

a. CSA approval is required before installing an IDS. Approval of a new IDS shall be based on the criteria of reference (n) or UL Standard 2050, reference (o), as determined by the CSA.

b. The UL listed Alarm Service Company (ASC) is responsible for completing the Alarm System Description Form.

ISL 2014-03 #2 (5-901). CSA Approval of IDS. DSS will approve the use of DoD intrusion detection systems (IDS) by cleared contractors who are located on DoD installations in lieu of a system that is UL-2050 certified when the following conditions are met:

- DSS serves as the CSO with oversight and inspection of the cleared contractor location as requested by the Heads of the DoD Component or Military Installation.
- the IDS system is approved by the Head of a DoD Component and documentation of the approval is provided to DSS;
- there is an agreement in place between the head of the installation and the cleared contractor that includes the procedures for alarm monitoring, investigative response; and maintenance of the IDS; and
- the cleared contractor maintains a copy of the above agreement.

5-902. Central Monitoring Station

ISL 2006-02 #19 (5-902). Intrusion Detection System (IDS) Monitoring Over Data Networks (ISL 05L-1 #11). Minimum acceptance criteria for the utilization of data networks for intrusion detection systems (IDS) are appended to this ISL. These criteria were developed in close coordination with representatives from industry, government and Underwriter's Laboratories (UL), and establish baseline security requirements for alarm system monitoring using data networks. These data networks may include private data networks (e.g., intranets or virtual private networks), or public data networks (e.g., the internet).

For the Department of Defense (DoD), all IDS equipment used to monitor classified information/equipment and sensitive arms, ammunitions and explosives, to include those utilizing data networks must be UL listed (in this case, UL listed to operate in a data network environment), and installed in accordance with UL standards. In addition, UL 2050 requires that any IDS utilizing data network monitoring must have the Cognizant Security Office (CSO) representative sign an Alarm System Description Form before a UL CRZH certificate will be issued. However, IDS approved by another government agency that meet DCID 6/9 standards may be accepted as outlined in the attachment to this ISL. *(See Appendix D for ISL Appendix, IDS Monitoring Over Data networks.)*

ISL 2014-03 #3 (5-902). NISPOM 5-902 states monitoring stations may be located at a UL-listed Government Contractor Monitoring Station (GCMS), cleared commercial central station, cleared protective signaling service station, or cleared residential monitoring station. In accordance with UL-2050 (National Industrial Security Systems), GCMSs are not required to be UL-listed. While GCMSs are not UL-listed, the UL-listed Alarm Services Company (ASC) verifies compliance with UL-2050 prior to issuing UL-2050 certificates for installed alarmed systems when monitored by the GCMS. The issuance of the UL-2050 certificate by the ASC for the installed alarm system serves as the documentation for approval and use of the GCMS by the contractor for the monitoring of alarms.

The fifth Edition of UL-2050, dated November 5, 2010 established the National Industrial Security Monitoring Station (NIMS) as a category of UL-Listed (CRZM) monitoring stations. The use of NIMS conforms to the requirements of NISPOM 5-902.

a. The central monitoring station may be located at a UL-listed: (1) Government Contractor Monitoring Station (GCMS), formerly called a proprietary central station; (2) cleared commercial central station; (3) cleared protective signal service station (e.g., fire alarm monitor); or (4) cleared residential monitoring station. For the purpose of monitoring alarms, all provide an equivalent level of monitoring service.

b. SECRET-cleared central station employees shall be in attendance at the alarm monitoring station in sufficient number to monitor each alarmed area within the cleared contractor facility.

c. The central monitoring station shall be required to indicate whether or not the system is in working order and to indicate tampering with any element of the system. Necessary repairs shall be made as soon as practical. Until repairs are completed, periodic patrols shall be conducted during non-working hours, unless a SECRET cleared employee is stationed at the alarmed site.

d. When an IDS is used, it shall be activated immediately at the close of business at the alarmed area or container. This may require that the last person who departs the controlled area or checks the security container notify the central monitoring station to set the alarm. A record shall be maintained to identify the person responsible for setting and deactivating the IDS. Each failure to activate or deactivate shall be reported to the FSO. Such records shall be maintained for 30 days.

e. Records shall be maintained for 90 days indicating time of receipt of alarm, name(s) of security force personnel responding, time dispatched to facility/area, time security force personnel arrived, nature of alarm, and what follow-up actions were accomplished.

5-903. Investigative Response to Alarms. The primary purpose of any alarm response team is to

ascertain if intrusion has occurred and if possible assist in the apprehension of the individuals involved. If an alarm activation resets in a reasonable amount of time and no damage to the area or container is visible, then entrance into the area or container is not required. Therefore, the initial response team may consist of uncleared personnel. If the alarm activation does not reset and damage is observed, then a cleared response team must be dispatched. The initial uncleared response team must stay on station until relieved by the cleared response team. If a cleared response team does not arrive within one hour, then a report to the CSA must be made by the close of the next business day.

a. The following resources may be used to investigate alarms: proprietary security force personnel, central station guards, or a subcontracted guard service.

(1) For a GCMS, trained proprietary or subcontractor security force personnel, cleared to the SECRET level and sufficient in number to be dispatched immediately to investigate each alarm, shall be available at all times when the IDS is in operation.

(2) For a commercial central station, protective signaling service station, or residential monitoring station, there shall be a sufficient number of trained guards available to respond to alarms. Guards shall be cleared only if they have the ability and responsibility to access the area or container(s) housing classified material; i.e., keys to the facility have been provided or the personnel are authorized to enter the building or check the container or area that contains classified material.

(3) Uncleared guards dispatched by a commercial central station, protective signaling service station, or residential monitoring station in response to an alarm shall remain on the premises until a designated, cleared representative of the facility arrives, or for a period of not less than 1 hour, whichever comes first. If a cleared representative of the facility does not arrive within 1 hour following the arrival of the guard, the central control station must provide the CSA with a report of the incident that includes the name of the subscriber facility, the date and time of the alarm, and the name of the subscriber's representative who was contacted to

respond. A report shall be submitted to the CSA within 24 hours of the next working day.

(4) Subcontracted guards must be under a classified contract with either the installing alarm company or the cleared facility.

b. The response time shall not exceed 15 minutes. When environmental factors (e.g., traffic, distance) legitimately prevent a 15-minute response time, the CSA may authorize up to a 30-minute response time. The CSA approval shall be documented on the UL Alarm System Description Form and the specified response time shall be noted on the alarm certificate. The UL standard for response within the time limits is 80%. That is the minimum allowable on-time response rate and anything less than 80% is unacceptable. However, in all cases, a guard or cleared employee must arrive at the alarmed premises.

5-904. Installation. The IDS at the facility, area or container shall be installed by a UL listed ASC or by a company approved by the CSA. When connected to a commercial central station, GCMS protective signaling service or residential monitoring station, the service provided shall include line security (i.e., the connecting lines are electronically supervised to detect evidence of tampering or malfunction), the extent of protection for a container shall be "Complete," and for an alarmed area shall be "Extent 3" as described in the reference (o) installation guide. CSA authorization on the Alarm System Description Form is required in the following circumstances:

a. Line security is not available. Installation will require two independent means of transmission of the alarm signal from the alarmed area to the monitoring station.

b. Alarm installation provides Extent 5 Protection. Reference (o) allows for Extent 5 based on patrolling guards and CSA approval of security-in-depth.

c. Law enforcement personnel are the primary alarm response. The contractor must obtain written assurance from the police department regarding the ability to respond to alarms.

d. Alarm signal transmission is over computer controlled data-networks (internet, intranet, etc.).

The CSA will provide specific acceptance criteria (e.g., encryption requirements, etc.) for alarms monitored over data networks.

e. Alarm investigator response time exceeds 15 minutes.

5-905. Certification of Compliance. Evidence of compliance with the requirements of this section will consist of a valid (current) UL Certificate for the appropriate category of service. This certificate will have been issued to the protected facility by UL, through the alarm installing company. The certificate serves as evidence that the alarm installing company: (a) is listed as furnishing security systems of the category indicated; (b) is authorized to issue the certificate of installation as representation that the equipment is in compliance with requirements established by UL for the class; and (c) is subject to the UL field countercheck program whereby periodic inspections are made of representative alarm installations by UL personnel to verify the correctness of certification practices.

5-906. Exceptional Cases

a. If the requirements set forth above cannot be met, the contractor may request CSA approval for an alarm system meeting one of the conditions listed below. CSA approval will be documented on the Alarm System Description Form.

(1) Monitored by a central control station but responded to by a local (municipal, county, state) law enforcement organization.

(2) Connected by direct wire to alarm receiving equipment located in a local (municipal, county, state) police station or public emergency service dispatch center. This alarm system is activated and deactivated by employees of the contractor, but the alarm is monitored and responded to by personnel of the monitoring police or emergency service dispatch organization. Personnel monitoring alarm signals at police stations or dispatch centers do not require PCLs. Police department response systems may be requested only when: (a) the contractor facility is located in an area where central control station services are not available with line security and/or proprietary security force personnel, or a contractually-dispatched response to an alarm signal cannot be

achieved within the time limits required by the CSA, and, (b) it is impractical for the contractor to establish a GCMS or proprietary guard force at that location. Nonetheless, installation of these systems must use UL-listed equipment and be accomplished by an ASC Service Center listed by UL for any of the following categories:

(a) Defense (National) Industrial Security Systems

(b) Proprietary Alarm Systems

(c) Central Station Burglar Alarm Systems

(d) Police - Station - Connected Burglar Alarm Systems

b. An installation proposal, explaining how the system would operate, shall be submitted to the CSA. The proposal must include sufficient justification for the granting of an exception and the full name and address of the police department that will monitor the

system and provide the required response. The name and address of the UL listed company that will install the system, and inspect, maintain, and repair the equipment, shall also be furnished.

c. The contractor shall require a 15-minute response time from the police department. Arrangements shall be made with the police to immediately notify a contractor representative on receipt of the alarm. The contractor representative is required to go immediately to the facility to investigate the alarm and to take appropriate measures to secure the classified material.

d. In exceptional cases where central station monitoring service is available, but no proprietary security force, central station, or subcontracted guard response is available, and where the police department does not agree to respond to alarms, and no other manner of investigative response is available, the CSA may approve cleared employees as the sole means of response.

CHAPTER 6

Visits and Meetings

Section 1. Visits

6-100. General. This section applies when, for a lawful and authorized U.S. Government purpose, it is anticipated that classified information will be disclosed during a visit to a cleared contractor or to a Federal facility.

6-101. Classified Visits. The number of classified visits shall be held to a minimum. The contractor must determine that the visit is necessary and that the purpose of the visit cannot be achieved without access to, or disclosure of, classified information. Contractors shall establish procedures to ensure positive identification of visitors, appropriate PCL, and need-to-know prior to the disclosure of any classified information. Contractors shall establish procedures to ensure that visitors are only afforded access to classified information consistent with the purpose of the visit.

6-102. Need-to-Know Determination. The responsibility for determining need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit. Need-to-know is generally based on a contractual relationship between the contractors. In other circumstances, disclosure of the information will be based on an assessment that the receiving contractor has a bona fide need to access the information in furtherance of a GCA purpose.

6-103. Visits by Government Representatives. Representatives of the Federal Government, when acting in their official capacities as inspectors, investigators, or auditors, may visit a contractor's facility, provided these representatives present appropriate government credentials upon arrival.

6-104. Visit Authorization

ISL 2006-01 #16 (6-104). The requirement for a visit authorization letter for classified visits within the Department of Defense is eliminated so long as the information necessary to verify the clearance of the visitor is available in JPAS and the contractor is able to determine the visitor's need-to-know. This does not apply to visits to or from other government

agencies (Department of Energy, State Department, Department of Homeland Security, Department of Justice/FBI, etc). Contractors must still submit visit authorization letters to non-DoD agencies.

Contractors can control only their own processes for receiving incoming notifications of classified visits. Contractors will have to comply with the classified visit requirements established by other contractors and DoD activities that their employees are visiting. Employees should be informed that they may have to provide their SSNs to either the host of a classified visit or to the receptionist/security officer of another contractor or DoD activity they will be visiting as part of the necessary clearance verification process.

When companies check the JPAS Person Summary screen for incoming visitors, they should:

- Verify the visitor's name and SSN.
- Check **current** access level to ensure the visitor can have access to the level of classified information to be disclosed.
- Check to ensure that the JPAS record shows a current affiliation with the contractor the visitor is representing.

As the contractor sponsoring the visit is not required to notify the site to be visited that the employee is no longer representing that contractor, a one-time check of JPAS for an on-going visit will not be sufficient. JPAS must be consulted regularly to ensure the access level and employment status of the visitor remains unchanged.

If a contractor is aware of locations that an employee frequently visits on a classified basis, and the employee is terminated, as a courtesy and in keeping with sound security practices, the contractor should notify the visited activities that the person is no longer employed or sponsored for visits.

The contractor should contact the DoD activities and other contractors prior to the scheduled arrival date of a visiting employee to determine how each organization wants to receive visitor data in order to verify the visitor's eligibility and access level. This will help ensure that employees are not denied entry.

ISL 2006-02 #20 (6-104). Visit Authorization Letters for the Department of Energy (DOE) (ISL 03L-1 #10). The Department of Energy requires requests for access to Restricted Data in the possession of DOE or other Federal Agencies designated by DOE to be made utilizing DOE Form 277, "Request for Visit or Access Approval." For contractors, the need for access to Restricted Data will, in all cases, be certified by a Government Contracting Officer (GCO). Failure to utilize the DOE Form 277 has caused unnecessary delays for some cleared contractor employees in gaining access to information required for job performance.

a. If a visit requires access to classified information, the host contractor shall verify the visitor's PCL level. Verification of a visitor's PCL may be accomplished by a review of a CSA-designated database that contains the information or by a visit authorization letter (VAL) provided by the visitor's employer.

ISL 2010-01 #5 (6-104.a). Release of JPAS records. JPAS, as a U.S. Government information system, contains official government records. The information in JPAS must be protected from unauthorized disclosure and used only for authorized purposes. Contractor personnel may only use their JPAS accounts to manage the access records of their company's employees and consultants, and to verify the access levels and employment affiliations of incoming visitors who require access to classified information. Contractor personnel are not authorized to, and may not, release printed or electronic copies of JPAS records to any person or entity. The appropriate U.S. Government release authority (commonly in an agency Privacy Act Office) is responsible for making release decisions regarding all JPAS records in accordance with the Privacy Act of 1974.

b. If a CSA-designated database is not available and a VAL is required, contractors shall include the following information in all VALs.

(1). Contractor's name, address, and telephone number, assigned Commercial and Government Entity (CAGE) code, if applicable, and certification of the level of the facility security clearance;

(2). Name, date and place of birth, and citizenship of the employee intending to visit;

(3). Certification of the proposed visitor's PCL and any special access authorizations required for the visit;

(4). Name of person(s) to be visited;

(5). Purpose and sufficient justification for the visit to allow for a determination of the necessity of the visit; and

(6). Date or period during which the VAL is to be valid.

6-105. Long-Term Visitors

a. When government employees or employees of one contractor are temporarily stationed at another contractor's facility, the security procedures of the host contractor will govern.

b. Government personnel assigned to or visiting a contractor facility and engaged in oversight of an acquisition program shall retain control of their work product. Classified work products of government employees shall be handled in accordance with this manual. Contractor procedures shall not require government employees to relinquish control of their work products, whether classified or not, to a contractor.

c. Contractor employees at government installations shall follow the security requirements of the host. However, this does not relieve the contractor from security oversight of their employees who are long-term visitors at government installations.

Section 2. Meetings

6-200. General. This section applies to a conference, seminar, symposium, exhibit, convention, training course, or other such gathering during which classified information is disclosed, hereafter called a "meeting."

6-201. Government Sponsorship of Meetings. Disclosure of classified information to large diverse audiences such as conferences increases security risks. However, classified disclosure at such meetings which serve a government purpose and at which adequate security measures have been provided in advance may be conducted by a cleared contractor provided the meeting is authorized by a government agency that has agreed to assume security jurisdiction. The government agency must approve security arrangements, announcements, attendees, and the location of the meeting. The government agency may delegate certain responsibilities to a cleared contractor for the security arrangements and other actions necessary for the meeting under the general supervision of the government agency.

a. **Requests for Authorization.** Contractors desiring to conduct meetings requiring sponsorship shall submit their requests to the Government Agency having principal interest in the subject matter of each meeting. The request for authorization shall include the following information:

(1) An explanation of the government purpose to be served by disclosing classified information at the meeting and why the use of conventional channels for release of the information will not advance those interests.

(2) The subject of the meeting and scope of classified topics, to include the classification level, to be disclosed at the meeting.

(3) The expected dates and location of the meeting.

(4) The general content of the proposed announcement and/or invitation to be sent to prospective attendees or participants.

(5) The identity of any other non-government organization involved and a full description of the type of support it will provide.

(6) A list of any foreign representatives (including their nationality, name, organizational affiliation) whose attendance at the meeting is proposed.

(7) A description of the security arrangements necessary for the meeting to comply with the requirements of this manual.

b. **Location of Meetings.** Classified sessions shall be held only at a Federal Government installation or a cleared contractor facility where adequate physical security and procedural controls have been approved. The authorizing government agency is responsible for evaluating and approving the location proposed for the meeting.

c. **Security Arrangements for Meetings.** The contractor shall develop the security measures and procedures to be used and obtain the authorizing agency's approval. The security arrangements must provide for the following:

(1) **Announcements.** Approval of the authorizing agency shall be obtained for all announcements of the meeting. Announcements shall be unclassified and shall be limited to a general description of topics expected to be presented, names of speakers, and administrative instructions for requesting invitations or participation. Classified presentations shall not be solicited in the announcement. When the meeting has been approved, announcements may only state that the government agency has authorized the conduct of classified sessions and will provide necessary security assistance. The announcement shall further specify that security clearances and justification to attend classified sessions are to be forwarded to the authorizing agency or its designee. Invitations to foreign persons shall be sent by the authorizing government agency.

(2) **Clearance and Need-to-know.** All persons in attendance at classified sessions shall possess the requisite clearance and need-to-know for

the information to be disclosed. Need-to-know shall be determined by the authorizing agency or its designee based on the justification provided. Attendance shall be authorized only to those persons whose security clearance and justification for attendance have been verified by the security officer of the organization represented. The names of all authorized attendees or participants must appear on an access list with entry permitted to the classified session only after verification of the attendee's identity based on presentation of official photographic identification such as a passport, contractor or U.S. Government identification card.

(3) **Presentations.** Classified information must be authorized for disclosure in advance by the government agency having jurisdiction over the information to be presented. Individuals making presentations at meetings shall provide sufficient classification guidance to enable attendees to identify what information is classified and the level of classification. Classified presentations shall be delivered orally and/or visually. Copies of classified presentations or slides, etc., shall not be distributed at the classified meeting, and any classified notes or electronic recordings of classified presentations shall be classified, safeguarded, and transmitted as required by this Manual.

(4) **Physical Security.** The physical security measures for the classified sessions shall provide for control of, access to, and dissemination of, the classified information to be presented and shall provide for secure storage capability, if necessary.

6-202. Disclosure Authority at Meetings. A contractor desiring to disclose classified information at a meeting shall:

a. Obtain prior written authorization for each proposed disclosure of classified information from the government agency having jurisdiction over the information involved.

b. Furnish a copy of the disclosure authorization to the government agency sponsoring the meeting.

c. Associations are not responsible for ensuring that classified presentations and papers of other organizations have been approved for disclosure. Authority to disclose classified information at meetings, whether disclosure is by officials of industry or government, must be granted by the government agency or activity that has classification jurisdiction over the information to be disclosed. Each contractor that desires to disclose classified information at a meeting is responsible for requesting and obtaining disclosure approvals.

6-203. Requests to Attend Classified Meetings. Before a contractor employee can attend a classified meeting, the contractor shall provide justification why the employee requires access to the classified information, cite the classified contract or GCA program/project involved, and forward the information to the authorizing government agency.

CHAPTER 7 Subcontracting

Section 1. Prime Contractor Responsibilities

7-100. General. This Chapter outlines the requirements and responsibilities of a prime contractor when disclosing classified information to a subcontractor.

7-101. Responsibilities. Before a prime contractor may release or disclose classified information to a subcontractor, or cause classified information to be generated by a subcontractor, the following actions are required:

ISL 2006-02 #6 (2-102 and 7-101). Facility Security Clearances (FCLs) for Service Contracts (ISL 05L-1 #8). DSS continues to receive requests to process companies for FCLs in order to perform service-oriented tasks (janitorial services for example). A fundamental requirement for FCL sponsorship is that the contractor must require access to classified information in connection with a legitimate U.S. Government or foreign government procurement. A request to clear a company solely to avoid implementing basic security procedures that would otherwise preclude access to classified information (e.g., escort by an authorized person in combination with appropriate area sanitization), is not justification for an FCL, and could lead to security vulnerability.

There may be rare exceptions when a company would genuinely need an FCL to perform service-oriented tasks. An example is when a cleaning company is under contract to clean an area that, due to the nature of the classified material involved, cannot be adequately sanitized to preclude access to classified information even with appropriate escort. In those rare exceptions, the letter to DSS sponsoring the company for an FCL must clearly explain the rationale for the FCL. Such requests will be carefully scrutinized, and the validity for maintaining the FCL, once granted, will be a point of emphasis during recurring DSS security reviews.

a. Determine the security requirements of the subcontract.

(1) Access to classified information will be required. This is a "classified contract" within the meaning of this Manual. A "security requirements clause" and a Contract Security Classification Specification shall be incorporated in the solicitation and in the subcontract (see the "security requirements clause" in the prime contract). The subcontractor must possess an appropriate FCL and safeguarding capability if possession of classified information will be required.

(a) If access will not be required in the pre-award phase, prospective subcontractors are not required to possess an FCL to receive or bid on the solicitation.

(b) If access will be required during the pre-award phase, all prospective subcontractors must possess the appropriate FCL and have safeguarding capability.

(2) Access to classified information will not be required. This is not a classified contract within the meaning of this Manual. If the prime contract contains requirements for release or disclosure of certain information even though not classified, such as sensitive but unclassified information, the requirements shall be incorporated in the solicitation and the subcontract.

b. Determine clearance status of prospective subcontractors.

(1) All prospective subcontractors have appropriate clearance. This determination can be made if there is an existing contractual relationship between the parties involving classified information of the same or higher category, by accessing the CSA-designated database, or by contacting the CSA.

(2) If a prospective subcontractor does not have the appropriate FCL or safeguarding capability, the prime contractor shall request the CSA of the subcontractor to initiate the necessary action. Requests shall include, as a minimum, the full name, address and contact information for the requester; the

full name, address, and contact information for a contact at the facility to be processed for an FCL; the level of clearance and/or safeguarding capability required; and full justification for the request. Requests for safeguarding capability shall include a description, quantity, end-item, and classification of the information related to the proposed subcontract. Other factors necessary to help the CSA determine if the prospective subcontractor meets the requirements of this manual shall be identified, such as any special access requirements.

c. Requesting contractors shall allow sufficient lead time in connection with the award of a classified subcontract to enable an uncleared bidder to be processed for the necessary FCL. When the FCL cannot be granted in sufficient time to qualify the prospective subcontractor for participation in the current procurement action, the CSA will continue the FCL processing action to qualify the prospective subcontractor for future contract consideration provided:

(1) The delay in processing the FCL was not caused by a lack of cooperation on the part of the prospective subcontractor;

(2) Future classified negotiations may occur within 12 months; and

(3) There is reasonable likelihood the subcontractor may be awarded a classified subcontract.

7-102. Security Classification Guidance. Prime contractors shall ensure that a Contract Security Classification Specification is incorporated in each classified subcontract. When preparing classification guidance for a subcontract, the prime contractor may extract pertinent information from the Contract Security Classification Specification issued with the prime contract; from security classification guides issued with the prime contract; or from any security guides that provide guidance for the classified information furnished to, or that will be generated by, the subcontractor. The Contract Security Classification Specification prepared by the prime contractor shall be certified by a designated official of the contractor. In the absence of exceptional

circumstances, the classification specification shall not contain any classified information. If classified supplements are required as part of the Contract Security Classification Specification, they shall be identified and forwarded to the subcontractor by separate correspondence.

a. An original Contract Security Classification Specification shall be included with each RFQ, RFP, IFB, or other solicitation to ensure that the prospective subcontractor is aware of the security requirements of the subcontract and can plan accordingly. An original Contract Security Classification Specification shall also be included in the subcontract awarded to the successful bidder.

b. A revised Contract Security Classification Specification shall be issued as necessary during the lifetime of the subcontract when the security requirements change.

c. Requests for public release by a subcontractor shall be forwarded through the prime contractor to the GCA.

7-103. Responsibilities (Completion of the Subcontract). Upon completion of the subcontract, the subcontractor may retain classified material received or generated under the subcontract for a 2-year period, provided the prime contractor or GCA does not advise to the contrary. If retention is required beyond the 2-year period, the subcontractor must request written retention authority through the prime contractor to the GCA. If retention authority is approved by the GCA, the prime contractor will issue a final Contract Security Classification Specification, annotated to provide the retention period and final disposition instructions.

7-104. Notification of Unsatisfactory Conditions. The prime contractor shall be notified if the CSA discovers unsatisfactory security conditions in a subcontractor's facility. When so notified, the prime contractor shall follow the instructions received relative to what action, if any, should be taken in order to safeguard classified material relating to the subcontract.

CHAPTER 8 Information System Security

Section 1. Responsibilities and Duties

8-100. General

a. Information systems (IS) that are used to capture, create, store, process or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information, loss of data integrity to ensure the availability of the data and system.

ISL 2007-01 #2 (8-100.a., 8-400). NISPOM Paragraph 8-100a states that the IS must be properly managed to protect against loss of data integrity and to ensure the availability of the data and system. Is paragraph 8-100a a statement of general security concerns or is it a National Industrial Security Program Operating Manual (NISPOM) requirement?

Answer: Paragraph 8-100a states a baseline standard. As stated in paragraph 8-400, the Government Contracting Activity (GCA)) will issue additional guidance or requirements if there is a need for data integrity and system availability controls.

b. Protection requires a balanced approach including IS security features to include but not limited to, administrative, operational, physical, computer, communications, and personnel controls. Protective measures commensurate with the classification of the information, the threat, and the operational requirements associated with the environment of the IS are required.

ISL 2007-01 #1 (5-306, 8-100.b.). Must classified materials incidental to the operation of Information Systems (IS) maintained in the Closed Area be stored in GSA approved containers?

Answer: Classified material, which includes magnetic and electronic media as well as printed materials, are normally to be stored in approved security containers within the Closed Area during non-working hours or when the area is unattended unless the area has been approved for open shelf or bin storage in accordance with NISPOM paragraph 5-306b. Large items essential to the operation of an IS do not need to be secured in approved security

containers in the Closed Area, provided all personnel with access to the Closed Area have the clearance and need-to-know for all classified information within the Closed Area. Examples of items that do not need to be stored in security containers inside the Closed Area include large removable hard drives that are not easily disconnected from the IS or physically moved, or can be damaged by constant removal, or other media and technical manuals that need to be readily accessible for ongoing classified processing.

c. The requirements outlined in the following sections apply to all information systems processing classified information. Additional requirements for high-risk systems and data are covered in the NISPOM Supplement.

ISL 2007-01 #33 (8-400, 8-100.c.). NISPOM Paragraph 8-100.c. states that "additional requirements for high-risk systems and data are covered in the NISPOM Supplement." What is the definition of "high-risk" systems and data? What are the security requirements for contractors who need to develop systems at PL 4?

Answer: A high-risk system is one that requires protection above the NISPOM baseline (i.e., multi-level) where high-risk data would be Special Access Program (SAP) or Special Compartment Information (SCI) information. Standards for SAP and SCI are typically established in contract documents by the responsible GCA.

8-101. Responsibilities

a. The CSA shall establish a line of authority for training, oversight, program review, certification, and accreditation of IS used by contractors for the processing of classified information. The CSA will conduct a risk management evaluation based on the contractor's facility, the classification, and sensitivity of the information processed. The evaluation must ensure that a balanced, cost-effective application of security disciplines and technologies is developed and maintained.

ISL 2009-01 #1 (8-101.a., 8-610.a.(1)(b)(3)). This Industrial Security Letter (ISL) pertains to the Defense Security Service (DSS) Office of Designated Approving Authority (ODAA) “Manual for the Certification and Accreditation of Classified Systems under the National Industrial Security Program Operating Manual (NISPOM),” hereafter referred to as the “Manual.”

Use of the Manual will support contractor compliance with the NISPOM. The Manual sets forth guidance for contractors to use in developing their system security plans (SSPs) and continuous certification and accreditation requirements. The Manual implements and conforms to NISPOM requirements, and is based on other Federal standards* that apply to national security systems used by Government and contractors. Use of, and adherence to, the Manual will facilitate the DSS review of SSPs and IS certifications.

**These standards include: Department of Defense (DoD), National Security Agency (NSA), Defense Information System Agency (DISA), National Institute of Standards and Technology (NIST), and the Committee on National Security Systems (CNSS).*

The CNSS (see National Security Directive Number 42, and Executive Order (EO) 13231, October 16, 2001) is chaired by the Department of Defense and is charged with setting national policy, operational procedures and guidance for National Security Systems (NSS). The CNSS goal was a convergence of standards for the DoD, Intelligence, and civilian communities into one common, consistent process with one set of common standards for the federal security authorization process (i.e., certification and accreditation). Contractor IS used to process classified information are defined as national security systems (NSS) per the Federal Information Security Management Act (FISMA) of 2002 (44 U.S.C. §3541, et seq., which refers to the definition of NSS at 44 U.S.C. §3532(b)(2)).

By FISMA definition, NSS are those that are used or operated by an agency or by a contractor of an agency, or another organization on behalf of the agency, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of

a weapon system, or are protected at all times by procedures established for information that have been specifically authorized under criteria established by an EO or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

The CNSS is also currently drafting the set of standards for NSS in draft CNSS Instruction 1253, “Security Control Catalog for National Security Systems”. These CNSS security standards and guidelines are integrated into a risk management framework that promotes the concept of “near real-time risk management” based on continuous monitoring of information systems. As contractor IS used to process classified information are considered to be NSS, DSS anticipates that these CNSS standards will form the basis of any future revisions to NISPOM requirements pertaining to IS security.

ISL 2009-01 #2 (8-101.a., 8-202, Chapter 8 Section 6). This Industrial Security Letter (ISL) pertains to the DSS ODAA “Standardization of Baseline Technical Security Configurations,” hereafter referred to as the “Baseline Standards.”

In accordance with its National Industrial Security Program oversight responsibilities, and as provided for in NISPOM 8-202, DSS has established an approved set of technical safeguards that DSS will apply in making a decision to accredit an IS. These technical safeguards are set forth in the Baseline Standards. The technical configurations prescribed in the Baseline Standards conform to NISPOM protection requirements (Section 6 of Chapter 8), as well as to Federal standards that apply to Government systems.

Using the baseline set of safeguards in the Baseline Standards will assist contractors in meeting their requirement to select, test, certify and document that a baseline of technical security controls has been implemented.

Contractor application of the safeguards in the Baseline Standards will facilitate the DSS decision to accredit an IS; that is, for DSS to take a risk-management approach to authorize an IS to operate in accordance with a specific set of baseline security settings for a specific IS in a specific environment and explicitly accepting the residual risk.

The Baseline Standards is available on the DSS website: www.dss.mil.

b. Contractor management will publish and promulgate an IS Security Policy addressing the classified processing environment. Additionally, an IS Security Manager (ISSM) will be appointed with oversight responsibility for the development, implementation, and evaluation of the facility's IS security program. Contractor management will assure that the ISSM is trained to a level commensurate with the complexity of the facility's IS.

ISL 2007-01 #3 (8-101.b.). Must the Information Systems Security Manager (ISSM) be an employee of the contractor?

Answer: Yes, the ISSM must be an employee of the contractor. Under certain circumstances (e.g., the corporate family operates in the same fashion as a multiple facility organization) and subject to DSS approval, the ISSM may be an employee of another cleared entity within the contractor's corporate family.

ISL 2007-01 #4 (8-101.b., 8-103). In a multiple facility organization (MFO), can an ISSM who has been granted self-certification authority self-certify systems across the MFO structure?

Answer: The ISSM who has been granted self-certification authority for like systems under approved Master System Security Plans (MSSP) may self-certify systems for those facilities where he or she has been designated as the ISSM. Within an MFO, contractor management can appoint an employee to serve as the ISSM for multiple facilities if the following conditions are met:

- Facilities are in close proximity to, or within a reasonable commuting distance from, the ISSM's duty station (Note: DSS will consider exceptions to this reasonable distance criteria on a case by case basis. Such requests must specify how the ISSM will carry out oversight and other responsibilities from afar).
- The aggregate complexity of the collective facilities is such that only one ISSM is required.
- The ISSM is trained to a level commensurate with the overall complexity of all facilities.

- Each facility has at least one appointed Information System Security Officer (ISSO) who has been assigned the duties identified in paragraph 8-104.

There are no restrictions on an experienced ISSM assisting another ISSM in a different geographical location but the local ISSM is responsible for the local system and must meet the requirements for self-certification. Emergency situations will be reviewed by DSS on a case-by-case basis.

ISL 2007-01 #5 (8-101.b.). What training should the ISSM receive and how will management ensure the requirement is met?

Answer: Contractor management is required to ensure that the ISSM is trained commensurate with the complexity of the systems managed. Contractors should take advantage of available courses such as the Defense Security Service (DSS) Academy NISPOM Chapter 8 Implementation Course to train the ISSM. The ISSM can also arrange to take any recognized or government agency IS security courses.

8-102. Designated Accrediting/Approving Authority. The CSA is the Designated Accrediting/Approving Authority (DAA) responsible for accrediting information systems used to process classified information in industry

ISL 2007-01 #6 (8-102). NISPOM paragraph 8-102 states the Cognizant Security Agency (CSA) is the Designated Approving Authority (DAA) responsible for accrediting IS used to process classified information. Can you elaborate on the responsibilities of the DAA position?

Answer: Within the National Industrial Security Program (NISP), the DAA is the government official with the authority to formally accredit operation of the contractor's IS for processing classified information. The DAA determines that the protection measures the contractor has identified in their System Security Plan (SSP) will effectively protect classified information. The DSS ODAA is the DAA for IS used to process classified information in cleared contractor facilities under DSS cognizance.

8-103. IS Security Manager (ISSM). The ISSM:

ISL 2007-01 #4 (8-101.b., 8-103). In a multiple facility organization (MFO), can an ISSM who has been granted self-certification authority self-certify systems across the MFO structure?

Answer: The ISSM who has been granted self-certification authority for like systems under approved Master System Security Plans (MSSP) may self-certify systems for those facilities where he or she has been designated as the ISSM. Within an MFO, contractor management can appoint an employee to serve as the ISSM for multiple facilities if the following conditions are met:

- Facilities are in close proximity to, or within a reasonable commuting distance from, the ISSM's duty station (Note: DSS will consider exceptions to this reasonable distance criteria on a case by case basis. Such requests must specify how the ISSM will carry out oversight and other responsibilities from afar).
- The aggregate complexity of the collective facilities is such that only one ISSM is required.
- The ISSM is trained to a level commensurate with the overall complexity of all facilities.
- Each facility has at least one appointed Information System Security Officer (ISSO) who has been assigned the duties identified in paragraph 8-104.

There are no restrictions on an experienced ISSM assisting another ISSM in a different geographical location but the local ISSM is responsible for the local system and must meet the requirements for self-certification. Emergency situations will be reviewed by DSS on a case-by-case basis.

a. Ensures the development, documentation, and presentation of IS security education, awareness, and training activities for facility management, IS personnel, users, and others, as appropriate.

b. Establishes, documents, implements, and monitors the IS Security Program and related procedures for the facility and ensures facility compliance with requirements for IS.

c. Identifies and documents unique local threats/vulnerabilities to IS.

d. Coordinates the facility IS Security Program with other facility security programs.

e. Ensures that periodic self-inspections of the facility's IS Program are conducted as part of the overall facility self-inspection program and that corrective action is taken for all identified findings and vulnerabilities. Self-inspections are to ensure that the IS is operating as accredited and that accreditation conditions have not changed.

f. Ensures the development of facility procedures to:

ISL 2007-01 #54 (5-704, 5-705, 8-103.f., 8-301). Can DSS provide guidance on the clearing and sanitization requirements for classified material no longer required?

Answer. Yes, DSS has published the following updated DSS Clearing and Sanitization Matrix on the DSS web site (www.dss.mil) under the Industrial Security Program tab. (See Paragraph 8-301 for ISL matrix.)

(1) Govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information.

(2) Properly implement vendor supplied authentication (password, account names) features or security-relevant features.

(3) Report IS security incidents to the CSA. Ensure proper protection or corrective measures have been taken when an incident/vulnerability has been discovered.

(4) Require that each IS user sign an acknowledgment of responsibility for the security of the IS.

(5) Implement security features for the detection of malicious code, viruses, and intruders (hackers), as appropriate.

ISL 2007-01 #27 (8-305, 8-103.f.(5)). What are the NISPOM security requirements for protection against malicious code in IS?

Answer: NISPOM requires that all IS, regardless of the OS, are protected against malicious code. The ISSM must implement policies and procedures that detect and deter incidents caused by malicious code, viruses, intruders, or unauthorized modifications to software or hardware. The IS must employ the appropriate software to check all files for viruses and malicious code before being introduced on an IS.

g. Certifies to the CSA, in writing, that each System Security Plan (SSP) has been implemented; that the specified security controls are in place and properly tested; and that the IS is functioning as described in the SSP.

h. Ensures notification of the CSA when an IS no longer processes classified information, or when changes occur that might affect accreditation.

i. Ensures that personnel are trained on the IS's prescribed security restrictions and safeguards before they are initially allowed to access a system.

j. Develops and implements general and remote maintenance procedures based on requirements provided by the CSA.

8-104. Information System Security Officer(s) (ISSO). ISSOs may be appointed by the ISSM in facilities with multiple accredited IS. The ISSM will determine the responsibilities to be assigned to the ISSO that may include the following:

a. Ensure the implementation of security measures, in accordance with facility procedures.

b. Identify and document any unique threats.

c. If so directed by the GCA and/or if an identified unique local threat exists, perform a risk assessment to determine if additional countermeasures beyond those identified in this chapter are required.

d. Develop and implement a certification test as required by the ISSM/CSA.

ISL 2007-01 #7 (8-104.d., 8-614). Paragraph 8-104.d. requires that an IS certification test be developed and implemented. What is a certification test and when would it be required?

Answer: A certification test or process outlines the inspection and test procedures used to demonstrate compliance with the security requirements associated with the Protection Level (PL) assigned to the IS. The certification test is administered during the certification process and verifies correct operation of the protection measures in the IS. When the ISSM signs the Certification Test, he/she is affirming in writing that the system is currently installed and configured as described in the SSP. The DSS accreditation decision relies heavily on the accuracy of the ISSM's certification.

e. Prepare, maintain, and implement an SSP that accurately reflects the installation and security provisions.

f. Notify the CSA (through the ISSM) when an IS no longer processes classified information, or when changes occur that might affect accreditation.

g. Ensure:

(1) That each IS is covered by the facility Configuration Management Program, as applicable.

(2) That the sensitivity level of the information is determined prior to use on the IS and that the proper security measures are implemented to protect this information.

(3) That unauthorized personnel are not granted use of, or access to, an IS.

(4) That system recovery processes are monitored to ensure that security features and procedures are properly restored.

h. Document any special security requirement identified by the GCA and the protection measures implemented to fulfill these requirements for the information contained in the IS.

i. Implement facility procedures:

(1) To govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information.

(2) To ensure that vendor-supplied authentication (password, account names) features or security-relevant features are properly implemented.

(3) For the reporting of IS security incidents and initiating, with the approval of the ISSM, protective or corrective measures when a security incident or vulnerability is discovered.

(4) Requiring that each IS user sign an acknowledgment of responsibility for the security of IS and classified information.

(5) For implementing and maintaining security-related software for the detection of malicious code, viruses, and intruders (hackers), as appropriate.

j. Conduct ongoing security reviews and tests of the IS to periodically verify that security features and operating controls are functional and effective.

k. Evaluate proposed changes or additions to the IS, and advises the ISSM of their security relevance.

l. Ensure that all active user IDs are revalidated at least annually.

ISL 2007-01 #8 (8-104.l., 8-303.g.). These paragraphs require that active user IDs be revalidated at least annually. Is there a requirement to revalidate users of standalone workstations or small local area networks (LAN) since user IDs are not required?

Answer: Yes, users of standalone workstations and LANs must be validated at least annually to verify that all users have a continued need to access the accredited IS. Access control lists (i.e., physical access) may be used if the IS does not require User IDs under 8-303c. If access control lists are used for revalidation, then the access control lists must be retained as an Audit 1 requirement as well as clearly identified in the system security plans. An on-going account management program is one of the basic tenets of IS security.

8-105. Users of IS. Users of IS are either privileged or general users.

a. Privileged users have access to IS control, monitoring or administration functions. Examples include:

ISL 2007-01 #19 (8-105.a., 8-302.a.). Are contractor employees who test commercially procured or security related software on an accredited classified system or a system in development that will process classified information required to have a clearance?

Answer: Yes. They are "privileged users" and require a security clearance at least equal to the level at which the IS is accredited.

(1) Users having "superuser," "root," or equivalent access to a system (e.g., system administrators, computer operators, ISSOs); users with near or complete control of an IS or who set up and administer user accounts and authenticators.

(2) Users having access to change control parameters (routing tables, path priorities, addresses, etc.) on routers, multiplexers, and other key IS equipment.

(3) Users who have been given the authority to control and change other users' access to data or program files (e.g., applications software administrators, administrators of specialty file systems, database managers).

(4) Users who have been given special access for troubleshooting or monitoring an IS' security functions (e.g., those using analyzers, management tools).

b. General users are individuals who can input information to or modify information on an IS or who can receive information from an IS without a reliable human review.

c. All users shall:

(1) Comply with the IS Security Program requirements.

(2) Be aware of and knowledgeable about their responsibilities in regard to IS security.

(3) Be accountable for their actions on an IS.

(4) Ensure that any authentication mechanisms (including passwords) issued for the control of their access to an IS are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access.

(5) Acknowledge, in writing, their responsibilities for the protection of the IS and classified information.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 2. Certification and Accreditation

8-200. Overview. The certification and accreditation (C&A) process is an integral part of the life cycle of an IS. The identification of protection measures occurs during system design or development. The formal C&A occurs after the protection measures have been implemented and any required IS protection documentation has been approved. Certification validates that the protection measures described in the SSP have been implemented on the system and that the protection measures are functioning properly. Accreditation is the approval by the CSA for the system to process classified information.

8-201. Certification Process. Certification is the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements. The certification process subjects the system to appropriate verification that protection measures have been correctly implemented. The ISSM shall review and certify to the CSA that all systems have the appropriate protection measures in place and validate that they provide the protection intended. The CSA may conduct an onsite assessment to validate the ISSM's review and certification of the IS.

ISL 2007-01 #9 (8-201, 8-610.a.). These paragraphs requires the ISSM to certify that their IS have undergone a comprehensive evaluation of all technical and non-technical security features and safeguards. Is this all that is required for certification?

Answer: For the ISSM's certification, yes. However, to make such a certification, the ISSM must ensure that all other NISPOM required signatures identified in 8-610.a. as a Doc 1 requirement have been included. In addition, DSS can require an on-site validation of the ISSM's certification prior to the final accreditation of the system.

ISL 2007-01 #14 (8-201, 8-202). What are the parameters for self-certification by a contractor?

The certification and accreditation processes are discussed in NISPOM paragraphs 8-201 and 8-202, respectively. The following discussion is an effort to make clear how DSS applies these terms.

Certification is the attestation by a contractor that comprehensive technical and non-technical system security controls are established and operating in conformity to a specified set of NISPOM security requirements. Certification of an IS is performed by the contractor in order to achieve accreditation from the Government.

Accreditation is the official governmental action performed by the DSS ODAA to permit an IS to operate at an acceptable risk level within a specified environment. Accreditation is issued after the contractor provides a certification that security controls are in place and operating as intended. All IS certifications shall be reviewed and IS accredited to operate by DSS (ODAA).

Self-Certification

Certification and accreditation of similar systems, commonly referred to as self-certification, is discussed in NISPOM paragraph 8-202.g. When specifically authorized in writing by DSS, an ISSM may extend an existing DSS accreditation to (i.e., self-certify) similar systems. ISSMs may self-certify similar systems only within specified parameters.

The general rules and parameters for self-certification are:

a) Self-certification must be based on a DSS-approved Master System Security Plan (MSSP). WANs and WAN interconnections (adding a node to a Network Security Plan) cannot be self-certified.

b) Any self certified system must be in compliance with applicable NISPOM requirements.

c) If a contractor is uncertain of the self-certification authority granted to them by DSS, the contractor should consult with DSS ODAA about the extent of their authority.

d) All required documentation for self-certified systems must be readily available for DSS review as detailed in the DSS ODAA Process Guide.

e) Self-certification authority is granted by DSS to a specific person at a particular CAGE Code in the Approval to Operate (ATO) letter. Self-certification

of systems outside of the CAGE Code specified in the ATO is not permitted.

The following table provides parameters governing self-certification by industry under a DSS-approved MSSP.

Table for self-certification
 (most common parameters)

	Protection Level (PL) (Note: 1)	Level of Concern (Note: 2)	Physical (Note: 3)	Operating Systems (OS) (Note: 4)	System Type (Note: 5)	Trusted Downloading Procedures (Note: 6)	Periods Processing (Note: 7)	Mobile Systems/ Alt Site (Note: 8)	Test Equipment (Note: 9)
Required to be considered "similar"	☒	☒	☒	☒	☒	☒	☒	☒	☒

Note: 1 – MSSP can consist of systems at PL-1 or PL-2, but not both.

Note: 2 – Level of Concern (NISPOM 8-401) must be the same. This refers to the classification levels of information (Top Secret, Secret, and Confidential)

Note: 3 – Physical. This pertains to the physical security environment (most notably restricted areas and closed areas). Be mindful that there are many scenarios that could describe a restricted area. Therefore, if the scenarios are not similar the IS will not be self-certified. In this case a reaccreditation of the MSSP would be required to include the additional scenario. There are hybrids (i.e. A LAN that encompasses closed and restricted areas) but are generally the exception rather than the rule.

Note: 4 – Only approved OS can be used for subsequent self-certified systems. However, a new OS can be added to an approved Protection Profile provided it's been previously approved by ODAA under another Protection Profile or Master Plan. In addition, any OS version changes may not be self-certified if the new version changes an approved existing security configuration. For clarification please check with ODAA for determination.

Note: 5 – System Type generally refers to system architecture: For example, Multi-user standalones (MUSA) or LANs. It can also refer how an IS is used. A Windows 2003 Server can be used as a Domain Controller (which controls half the (I&A)

"handshake" and requires all technical security features to be enabled) or as a file server (which can be recognized as a pure server in some instances which doesn't require all technical security features to be enabled).

Note: 6 – TDP (Trusted Downloading Procedures). Only the DSS approved procedures can be considered for self-certification.

Note: 7 – Periods Processing (NISPOM 8-502). Periods processing provides the capability to either have more than one user or group of users (sequentially) on a single-user IS who do not have the same need-to-know or who are authorized to access different levels of information; or use an IS at more than one protection level (sequentially).

Note: 8 – Mobile Systems. Procedures for identifying, managing and protecting mobile systems must be similar for DSS to consider approving self-certification.

Note: 9 – Test equipment can only be self-certified if it is the same make and model as another device that has been previously accredited by DSS.

8-202. Accreditation. The accreditation of an IS is the official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of a CSA approved set of technical, managerial and procedural

safeguards. All IS certifications shall be reviewed and IS accredited to operate by the CSA.

ISL 2007-01 #10 (8-202, 8-610). Is a Memorandum of Understanding (MOU) required when accredited mobile systems are relocated to government activities or test sites?

Answer: The contractor must have a signed letter from the GCA acknowledging acceptance of the relocation of the IS to the Government Activity prior to shipment. An MOU is not necessary unless the mobile system is connecting to an accredited government system.

ISL 2009-01 #2 (8-101.a., 8-202, Chapter 8 Section 6). This Industrial Security Letter (ISL) pertains to the DSS ODAA “Standardization of Baseline Technical Security Configurations,” hereafter referred to as the “Baseline Standards.”

In accordance with its National Industrial Security Program oversight responsibilities, and as provided for in NISPOM 8-202, DSS has established an approved set of technical safeguards that DSS will apply in making a decision to accredit an IS. These technical safeguards are set forth in the Baseline Standards. The technical configurations prescribed in the Baseline Standards conform to NISPOM protection requirements (Section 6 of Chapter 8), as well as to Federal standards that apply to Government systems.

Using the baseline set of safeguards in the Baseline Standards will assist contractors in meeting their requirement to select, test, certify and document that a baseline of technical security controls has been implemented.

Contractor application of the safeguards in the Baseline Standards will facilitate the DSS decision to accredit an IS; that is, for DSS to take a risk-management approach to authorize an IS to operate in accordance with a specific set of baseline security settings for a specific IS in a specific environment and explicitly accepting the residual risk.

The Baseline Standards is available on the DSS website: www.dss.mil.

a. Interim Approval to Operate. The CSA may grant interim approval (temporary authority) to operate an IS. Interim approval to operate may be granted for up to 180 days with an option for the CSA to extend the interim approval for an additional 180 days. CSA-approved protection measures shall be in place and functioning during the period of interim approval.

b. Reaccreditation. IS shall be reaccredited whenever security relevant changes are made to the accredited IS. Proposed modifications to an IS shall be reviewed by the ISSM to determine if the proposed modifications will impact the protections on the system. If the protection aspects of the system’s environment change, if the applicable IS protection requirements change, or if the protection mechanisms implemented for the system change, the system shall be reaccredited. During the reaccreditation cycle, the CSA may grant an interim approval to operate the system.

c. Review of Security-Relevant Changes. All modifications to security-relevant resources (including software, firmware, hardware, or interfaces and interconnections to networks) shall be reviewed and approved in accordance with procedures prior to implementation. All security-relevant changes shall be subject to the provisions of the system configuration management program. The ISSM shall notify the CSA of requests for changes to the resources that deviate from the requirements of the approved SSP. The CSA shall determine if system reaccreditation is required.

ISL 2007-01 #11 (8-202.c., 8-202.d., 8-202.e., 8-202.f.). Who is responsible for re-evaluating the IS, tracking the IATO and requesting re-accreditation prior to the end of the three (3) year Approval to Operate (ATO)?

Answer: Expiration, withdrawal or invalidation of an accreditation are all events that mean the affected IS is not authorized to process classified information. It is the ISSM’s responsibility to:

a) Track and prepare for the expiration of the IATO.

b) Track and prepare for the expiration of the three (3) year ATO.

c) Track changes to the IS for compliance with the proposed SSP for the IATO.

d) Re-evaluate each IS for changes that would require re-accreditation (paragraph 8-202b).

e) Contact the DSS ODAA prior to the ATO accreditation expiration and notify the ODAA as to whether or not changes have been made to the IS.

d. Re-evaluation of an Accreditation. Each IS shall be re-evaluated for reaccreditation every 3 years. Such review involves a determination by the CSA, with input from the ISSM that the conditions under which the original accreditation was granted still apply. If the accreditation remains valid, the accreditation originally furnished by the CSA need only be annotated that the re-evaluation was conducted and the date of the re-evaluation.

e. Withdrawal of Accreditation. The CSA shall evaluate the risks and consider withdrawal of accreditation if the protection measures approved for the system do not remain effective or whenever any of the following items change: levels of concern, protection level, technical or nontechnical protection measures, vulnerabilities, operational environment, operational concept, or interconnections. The CSA shall withdraw accreditation and ensure proper sanitization when the system is no longer required to process classified information, or if the operational need for the system no longer outweighs the risk of operating the system.

f. Invalidation of an Accreditation. The CSA will be notified and an accreditation will become invalid immediately whenever detrimental, security-significant changes occur to any of the following: the required protection level; the operational environment; or the interconnections.

g. Certification and Accreditation of Similar Systems. If two or more similar IS are to be operated in equivalent operational environments (e.g., the levels of concern and protection level are the same, the users have at least the required clearances and access approvals for all information on the IS, the IS configurations are essentially the same, and the physical security requirements are similar), a Master SSP may be written by the ISSO, certified by the ISSM, and then approved by the CSA to cover all

such IS. The IS covered by a Master SSP may range from stand alone workstations up to and including multi-user IS and local networks that meet the criteria for a Master SSP approach. This type of approval applies only to systems operating at Protection Levels 1 and 2 (see 8-402).

ISL 2007-01 #12 (8-202.g.). Can one Master SSP (MSSP) cover multiple cleared facilities?

Answer: No. While many elements of an MSSP may be the same (for similar IS), each MSSP must be tailored to the unique circumstances of each cleared facility.

ISL 2007-01 #13 (8-202.g.). Can one MSSP be written that covers all IS within the contractor's facility that operate at PL 1 and PL 2?

Answer: No. Paragraph 8-202g states that the IS covered by a single MSSP must have equivalent operational environments, and PL1 and PL2 are distinct operational environments.

(1) Master Information Systems Security Plan. The Master SSP shall specify the information required for each certification for an IS to be accredited under the plan.

(2) An IS Certification Report shall contain the information system identification and location and a statement signed by the ISSM certifying that the IS implements the requirements in the Master SSP.

(3) The CSA shall accredit the first IS under the Master SSP. All other IS to be operated under the Master SSP shall be certified by the ISSM as meeting the conditions of the approved Master SSP. This certification, in effect, accredits the individual IS to operate under the Master SSP. A copy of each certification report shall be retained with the approved copy of the Master SSP.

ISL 2007-01 #15 (8-202.g.(3)). Paragraph 8-202.g.(3) requires the ISSM to certify additional IS under an MSSP but does not require notification to DSS. Should DSS be notified?

Answer: Yes. It's imperative that DSS have up-to-date knowledge and awareness of all accredited IS

processing classified information. At a minimum, the contractor shall provide an updated list of IS self-certified under an MSSP to the IS Rep and ISSP on a quarterly basis. If the IS Rep or ISSP determines that more frequent notification is necessary because of volume or complexity or to address specific security concerns, the IS Rep or ISSP can request more frequent notification.

(4) Recertification. IS certified under a Master SSP remain certified until the Master SSP is changed or 3 years have elapsed since the IS was certified. If either the levels of concern or protection

level described in the Master SSP change, the Master SSP shall be re-accredited by the CSA and all IS certified under the Master SSP shall be re-certified by the ISSM in coordination with the CSA.

h. **Systems under Multiple CSAs.** For a system that involves multiple CSAs, the CSAs shall designate a primary CSA. Each facility involved in the system shall identify, in writing, the security officials who are responsible for implementing IS protection on the system components at their respective facility.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 3. Common Requirements

8-300. Introduction. This section describes the protection requirements that are common to all IS.

8-301. Clearing and Sanitization. Instructions on clearing, sanitization and release of IS media shall be issued by the accrediting CSA.

ISL 2007-01 #54 (5-704, 5-705, 8-103.f., 8-301).
Can DSS provide guidance on the clearing and sanitization requirements for classified material no longer required?

Answer. Yes, DSS has published the following updated DSS Clearing and Sanitization Matrix on the DSS web site (www.dss.mil) under the Industrial Security Program tab. (See Paragraph 8-301 for ISL matrix.)

DSS Clearing and Sanitization Matrix (Updated June 28, 2007)

NISPOM paragraphs 5-704 and 5-705 set out requirements for the destruction of classified material that is no longer required, including media, memory, and equipment. The appropriate procedure to be used

is based on the classification sensitivity of the information and the type (size, capacity and coercivity) of the media. There is currently no overwriting product or process that has been evaluated in accordance with the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS).

Therefore, in accordance with NISPOM paragraph 8-301, DSS will apply the guidance in the NSA CSS Policy Manual 9-12, "NSA/CSS Storage Device Declassification Manual", dated 13 Mar 2006, to sanitization, declassification, and release of IS storage devices for disposal or recycling. Effective immediately, DSS will no longer approve overwriting procedures for the sanitization or downgrading (e.g. release to lower level classified information controls) of IS storage devices (e.g., hard drives) used for classified processing.

The matrix provides guidance regarding clearance, sanitization (destruction) and disposition of the most common media, memory and equipment used for classified processing.

Clearing and Sanitization Matrix¹

Media	Clear					Sanitize														
Magnetic Tape																				
Type I	a					b											1			
Type II	a					b											1			
Type III	a					b											1			
Magnetic Disk																				
Bernoullis	a	c				b											1			
Floppy	a	c				b											1			
Non-Removable Rigid Disk		c				a											1			
Removable Rigid Disk	a	c				a											1			
Optical Disk																				
Read Many, Write Many		c															1			
Read Only																	1	m		
Write Once, Read Many (Worm)																	1	m		
Memory																				
Dynamic Random Access Memory (DRAM)		c	g				c					g					1			
Electronically Alterable Programmable Read Only Memory (EAPROM)				h										i			1			
Electronically Erasable PROM (EEPROM)				h					f								1			

Erasable Programmable ROM (EPROM)				j		c							k	l			k then c
Flash EPROM (FEPROM)			h			c				h				l			c then h
Programmable ROM (PROM)		c												l			
Magnetic Bubble Memory		c			a	c								l			
Magnetic Core Memory		c			a		d							l			
Magnetic Plated Wire		c			a	c		e						l			c and e
Magnetic Resistive Memory		c												l			
Non-Volatile RAM (NOVRAM)		c				c								l			
Read Only Memory (ROM)														l			
Synchronous DRAM (SDRAM)		c	g			c			g					l			
Static Random Access Memory (SRAM)		c	g			c			g					l			
Equipment																	
Monitor			g													p	
Impact Printer			g						g						o		o then g
Laser Printer			g						g						n		

In addition, NIST Special Publication 800-88, Guidelines for Media Sanitization, dated Sep 2006, can assist organizations and system owners in making practical sanitization decisions based on the level of confidentiality of their information, ensuring cost effective security management of their IT resources, and mitigate the risk of unauthorized disclosure of information.

INSTRUCTIONS FOR READING THE MATRIX:

A letter in black in the above table indicates the procedure is a complete, single option, e.g. EEPROM sanitization: Perform either procedure g or l (refer to indices below) and the media/memory is completely sanitized. Letters in **red** indicate the procedures must be combined for a complete sanitization, e.g., Laser Printer sanitization: **n** must be performed, then **g**. Note: when a combination of two procedures is required, the far right hand column indicates the order of the procedures. e.g., **o then g**.

MATRIX INDEX:

- Degauss with Type I, II, or III degausser.
- Degauss with same Type (I, II, or III) degausser.
- Overwrite all addressable locations with a single character.
- Overwrite all addressable locations with a character, its complement, then a random character.
- Each overwrite must reside in memory for a period longer than the classified data resided.
- Overwrite all locations with a random pattern, then with binary zeros, and finally with binary ones.
- Remove all power to include battery power.

h. Perform a full chip erase as per manufacturer's data sheets.

i. Perform h above, then c above, a total of three times.

j. Perform an ultraviolet erase according to manufacturer's recommendation.

k. Perform j above, but increase time by a factor of three.

l. Destruction (see below.)

m. Destruction required only if classified information is contained.

n. Run 1 page (font test acceptable) when print cycle not completed (e.g. paper jam or power failure). Dispose of output as unclassified if visual examination does not reveal any classified information.

o. Ribbons must be destroyed. Platens must be cleaned.

p. Inspect and/or test screen surface for evidence of burn-in information. If present, screen must be destroyed.

Destruction Methods for Classified Media and Equipment:

A. NISPOM Paragraph 5-705 reflects requirements for destruction of classified material, including classified media and equipment. DSS recommends

methods and procedures for destroying classified media and equipment should be reflected in the System Security Plan and reviewed/approved in connection with the information system certification and accreditation process. The following summary information is provided for contractor facilities in updating system security procedures for destruction of classified media:

- Incineration is the most common and recommended method for removing recording surfaces.
- Applying an abrasive substance to completely remove the recording surface (e.g. emery wheel, disk sander, belt sander, sand blaster) from the magnetic disk or drum. Make certain that the entire recording surface has been thoroughly destroyed before disposal. Ensure proper protection from inhaling the abraded dust.
- Degaussing or destruction using government approved devices. NSA publishes guidance on the sanitization, declassification, and release of Information Systems (IS) storage devices for disposal or recycling in the NSA CSS Policy Manual 9-12, NSA/CSS Storage Device Declassification Policy Manual, dated 13 Mar 2006. It is recommended that prior to performing any process for disposal, recycling or release of storage, media, or equipment that users review the manual and/or check for any updates to the guidance. NSA publishes on a recurring basis, updated Evaluated Products Lists (EPL) for High Security Crosscut Paper Shredders, High Security Disintegrators and Optical Media Destruction Devices. Contractors may utilize NSA evaluated destruction devices for destruction of classified media and hardware without prior authorization from DSS. For use of non-NSA approved devices or procedures, prior approval of the CSA is required.
- Smelting, disintegrating, or pulverizing hard disks or drums at an approved metal destruction facility. Prior approval of the CSA is required.
- Destroying by the use of chemicals (e.g. application of concentrated hydriodic acid (55 to 58 percent solution). Chemical destruction is hazardous and should only be done by trained

personnel in a proper environment (e.g. licensed facility, well-ventilated area, safety equipment and procedures, etc.) Prior CSA approval is required.

- Due to the proliferation, wide spread use, interoperability, low cost of USB technologies throughout the Global Information Grid (GIG), USB media and equipment no longer required to store or process classified information must be destroyed.

B. The National Security Agency (NSA) Classified Material Conversion (CMC) destruction facility may be utilized by qualified and registered contractors. NSA CMC will accept all COMSEC hardware and materials (regardless of ownership), classified Government Furnished Equipment (GFE) (including media), and Special Access Program (SAP) information from contractor facilities, with the prior endorsement of a government contracting officer (CO) or contracting officer representative (COR) in accordance with NSA CMC contractor registration procedures reflected in NSA guidance "Contractor Request for NSA CDC Services". Guidance for registration for NSA destruction services is also available on the DSS website.

a. **Clearing.** Clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information.

ISL 2007-01 #16 (8-301.a., 8-501). Can DSS provide more guidance on when sanitization or clearing of memory and media is required?

Answer: Sanitization of memory and media is required when the memory or media is no longer needed to store classified information. Clearing is required before and after periods of processing as a method of ensuring need-to-know protection, and prior to maintenance. Clearing is all that is required when the memory or media will be used at a higher classification level or at a more restrictive information sensitivity level. The clearing and sanitization matrix is available on the DSS web site.

Users unable to access the matrix should contact their local DSS Industrial Security Representative.

b. **Sanitization.** Sanitization is the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was in the media before sanitizing. IS resources shall be sanitized before they are released from classified information controls or released for use at a lower classification level.

8-302. Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.

a. **IS Software.** Commercially procured software shall be tested to ensure that the software contains no obvious features that might be detrimental to the security of the IS. Security-related software shall be tested to verify that the security features function as specified.

ISL 2007-01 #17 (8-302.a.). What does an unclassified software review and/or testing encompass?

Answer: Paragraph 8-302a provides two options for examination of unclassified software prior to its introduction into the IS and use for classified processing. The contractor may choose either a review or testing of the unclassified software. An unclassified software review must be a line-by-line source code review. Unclassified software testing must include a verification of all functionality for security-relevant items (e.g., includes security relevant software such as all OS software on an IS where Identification and Authentication (I&A) and/or auditing have been technically implemented, virus and malicious code detection and sanitization software, all security relevant information such as software and router tables, configuration settings, IS and OS documentation, audit data, etc. Security relevant hardware includes any hardware or IS component that contains, or has the potential of containing classified information) as well as resolution of any discrepancies. For example, if the software writes to a file, the file must then be reviewed using a hexadecimal editor to ensure that only the intended information was written.

ISL 2007-01 #18 (8-302.a.). What are the review requirements for contractors that develop unclassified software that will be used during classified processing periods?

Answer: Unclassified software that will eventually be used during classified processing periods must either be developed by cleared, knowledgeable personnel or reviewed and/or tested by cleared, knowledgeable personnel. The review and/or testing is done to provide reasonable assurance that security vulnerabilities do not exist.

ISL 2007-01 #19 (8-105.a., 8-302.a.). Are contractor employees who test commercially procured or security related software on an accredited classified system or a system in development that will process classified information required to have a clearance?

Answer: Yes. They are “privileged users” and require a security clearance at least equal to the level at which the IS is accredited.

ISL 2007-01 #20 (8-302.a.). Can commercially procured or security related software be used to disconnect hardware components not used for classified processing or to configure the IS for a classified processing session?

Answer: Yes. Provided the IS is not accredited at the level of TOP SECRET and the procured security related software has been tested and operates as specified.

ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)(c)). Can DSS provide additional guidance on the trusted download process and the requirement for output and media review?

Answer: Yes, Due to the diversity and uniqueness of the numerous vendor platforms and applications in use (e.g., word processing, database, electronic mail, and spreadsheets), a thorough review by the ISSM and DSS must be conducted before the trusted downloading procedures are used to create classified or unclassified electronic files and/or media.

All trusted downloading procedures must use new media. This mitigates the possibility of classified

system contamination or corruption, as used media could contain and inadvertently introduce unauthorized software into the classified system.

The DSS Trusted Downloading Procedures can be found on the DSS web site (www.dss.mil) under the Industrial Security Program link. These procedures support many of the standard applications and can be used to examine information that is not in human readable form with the reasonable assurance that only the requested information was transferred.

If the ISSM is unable to implement the DSS procedures found on the DSS website, the System Security Plan (SSP) must (under the vulnerability reporting requirement of paragraph 8-610a(1)(c)) include a description of how and why the contractor has deviated from the standard, and a risk acceptance statement by the GCA.

Trusted Downloading Procedures do not need to be followed when classified information is transferred from an accredited PL 1 system storing the same level of classified information from multiple programs to media that will be handled and then remain at the same or higher level classified environment and controls (i.e., handling, marking, distribution/access controls, safeguarding, etc.). However, a review must be accomplished to ensure that only the designated files were transferred to the new media. This could include a review of hard copy output and/or a visual review of the electronic file.

b. IS Hardware. Hardware shall be examined to determine that it appears to be in good working order and has no elements that might be detrimental to the secure operation of the IS when placed under facility control and cognizance. Subsequent changes and developments that affect security may require additional examination.

8-303. Identification and Authentication Management. As the complexity of a specific IS and the associated residual risk for this system increase, the need for identification and authentication of users and process becomes more significant. Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system and shall be managed in accordance with procedures identified in the SSP.

a. Unique Identification. Each user shall be uniquely identified and that identity shall be associated with all auditable actions taken by that individual.

b. Authentication at Logon. Users shall be required to authenticate their identities at “logon” time by supplying their authenticator, such as a password, smart card, or biometrics, in conjunction with their user identification (ID) prior to the execution of any application or utility on the system.

c. Applicability of Logon Authentication. In some cases, it may not be necessary to use IS security controls as logon authenticators. In the case of stand alone workstations, or small local area networks, physical security controls and personnel security controls may suffice. For example, if the following conditions are met, it may not be necessary for the IS to have a logon and password:

ISL 2007-01 #23 (8-303.c). This paragraph permits physical security controls and personnel security controls to augment the logon authentication requirement for standalone workstations or local area networks (LANs). What types of personnel security controls are acceptable?

Answer: The ISSM/ISSO must ensure that all users meet clearance, formal access approval, and need-to-know requirements. GCA concurrence is required when technical logon controls (i.e., identification and authentication) are not established. These personnel controls are acceptable to meet or augment the logon authentication requirements for those systems. Once briefed, the users’ names should be added to the area access list or the equipment authorization list which authenticates that the users are authorized and briefed.

ISL 2007-01 #24 (8-303.c). This paragraph permits physical security and personnel security controls in place of logon authenticators for small local area networks (LANs). Does “small” refer to the number of workstations or the area in which the workstations reside?

Answer: “Small” refers to size of the area in which the workstations are located. The users and systems should be easily observable by the ISSO (e.g., within

the same room, group of cubicles, adjoining offices in close proximity to each other).

(1) The workstation does not have a permanent (internal) hard drive, and the removable hard drive and other associated storage media are stored in an approved security container when not in use.

(2) All of the users with access to the workstation and the security container/ removable media have the required clearance level and need-to-know for all of the data processed on the workstation.

(3) The workstation is located within an approved security area, and all uncleared/lower-cleared personnel are escorted within the area.

d. Access to Authentication Data. Access to authentication data shall be restricted to authorized personnel through the use of encryption or file access controls, or both.

e. User ID Reuse. Prior to reuse of a user ID, all previous access authorizations (including file accesses for that user ID) shall be removed from the system.

f. User ID Removal. When an employee terminates, loses access to the system for cause, or no longer has a reason to access the IS, that individual's user ID and its authentication shall be disabled or removed from the system.

g. User ID Revalidation. Active user IDs are revalidated at least annually.

ISL 2007-01 #8 (8-104.I., 8-303.g.). These paragraphs require that active user IDs be revalidated at least annually. Is there a requirement to revalidate users of standalone workstations or small local area networks (LAN) since user IDs are not required?

Answer: Yes, users of standalone workstations and LANs must be validated at least annually to verify that all users have a continued need to access the accredited IS. Access control lists (i.e., physical access) may be used if the IS does not require User IDs under 8-303c. If access control lists are used for revalidation, then the access control lists must be retained as an Audit 1 requirement as well as clearly

identified in the system security plans. An on-going account management program is one of the basic tenets of IS security.

h. Protection of Individual Authenticator. An authenticator that is in the form of knowledge (password) or possession (smart card, keys) shall not be shared with anyone.

i. Protection of Individual Passwords. When passwords are used as authenticators, the following shall apply:

ISL 2007-01 #22 (8-303.i.). Must BIOS Passwords meet the same NISPOM requirements as authenticator passwords?

Answer: Yes, BIOS passwords must meet the NISPOM length and complexity requirements. A waiver is not required if a system's BIOS passwords cannot be configured to meet the NISPOM requirement. However, a waiver must be requested if the system's BIOS cannot be password protected for operational reasons. BIOS passwords are not deemed user authenticators and need not be changed annually.

(1) Passwords shall be protected at a level commensurate with the sensitivity level or classification level and classification category of the information to which they allow access.

(2) Passwords shall contain a minimum of eight non-blank characters, shall be valid for no longer than 12 months and changed when compromised.

(3) Passwords shall be generated by a method approved by the CSA. Password acceptability shall be based on the method of generation, the length of the password, password structure, and the size of the password space. The password generation method, the length of the password, and the size of the password space shall be described in an attachment to the SSP.

ISL 2007-01 #25 (8-303.i.(3)). What method(s) of password generation will DSS approve?

Answer: The recommended method of password generation is for the IS to generate unique, random

passwords. User-generated passwords are permitted, but must be a minimum of eight characters that are a mix of alpha/numeric and upper/lower case characters. Users shall be briefed not to use dictionary definable words for passwords that include sport names, pets or family members. The SSP must address the password generation method, and whether the password is unique and random.

(4) When an IS cannot prevent a password from being echoed (e.g., in a half-duplex connection), an overprint mask shall be printed before the password is entered to conceal the typed password.

(5) User software, including operating system and other security-relevant software, comes with a few standard authenticators (e.g., SYSTEM, TEST, and MASTER) and passwords already enrolled in the system. The ISSO shall ensure that the passwords for all standard authenticators are changed before allowing the general user population access to the IS. The ISSO shall also ensure that these passwords are changed after a new system version is installed or after other action is taken that might result in the restoration of these standard passwords.

8-304. Maintenance. IS are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.

a. Cleared Maintenance Personnel. Maintenance personnel who are cleared to the highest classification level of information on the system and indoctrinated for all information processed on that system do not require an escort, if need-to-know controls can be implemented. When possible, an appropriately cleared and technically knowledgeable, facility employee shall be present within the area where the maintenance is being performed to ensure that security procedures are being followed.

b. Uncleared (or Lower-Cleared) Maintenance Personnel

(1) If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used, provided an

appropriately cleared and technically qualified escort monitors and records the maintenance person's activities in a maintenance log. Uncleared maintenance personnel must be U.S. citizens.

(2) System initiation and termination shall be performed by the escort. In addition, keystroke monitoring shall be performed during access to the system.

(3) Prior to maintenance, the IS shall be completely cleared and all non-volatile data storage media shall be removed or physically disconnected and secured. When a system cannot be cleared procedures, which are identified in the SSP, shall be enforced to deny the maintenance personnel visual and electronic access to any classified data contained on the system.

(4) A separate, unclassified copy of the operating system, including any micro-coded floppy disks, CD-ROM, or cassettes that are integral to the operating system, shall be used for all maintenance operations. The copy shall be labeled "UNCLASSIFIED -- FOR MAINTENANCE ONLY" and protected in accordance with procedures established in the SSP. Maintenance procedures for an IS using a non-removable storage device on which the operating system is resident shall be considered by the ISSM on a case-by-case basis.

ISL 2007-01 #26 (8-304.b.(4)). This paragraph states that a separate copy of the operating system must be used during maintenance operations. If the contractor has arranged for remote maintenance, can the original operating system that is used for classified processing stay resident on-line during the maintenance operation?

Answer: No. The contractor performing maintenance must use a separate copy of the operating system and any maintenance software. As an exception, the ISSM may consider using alternate maintenance procedures for remote maintenance by contractors in accordance with the SSP using an on-line operating system.

8-305. Malicious Code. Policies and procedures to detect and deter incidents caused by malicious code, such as viruses or unauthorized modification to software, shall be implemented. All files must be

checked for viruses before being introduced on an IS and checked for other malicious code as feasible. The use of personal or public domain software is strongly discouraged. Each installation of such software must be approved by the ISSM.

ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)(c)). Can DSS provide additional guidance on the trusted download process and the requirement for output and media review?

Answer: Yes, Due to the diversity and uniqueness of the numerous vendor platforms and applications in use (e.g., word processing, database, electronic mail, and spreadsheets), a thorough review by the ISSM and DSS must be conducted before the trusted downloading procedures are used to create classified or unclassified electronic files and/or media.

All trusted downloading procedures must use new media. This mitigates the possibility of classified system contamination or corruption, as used media could contain and inadvertently introduce unauthorized software into the classified system.

The DSS Trusted Downloading Procedures can be found on the DSS web site (www.dss.mil) under the Industrial Security Program link. These procedures support many of the standard applications and can be used to examine information that is not in human readable form with the reasonable assurance that only the requested information was transferred.

If the ISSM is unable to implement the DSS procedures found on the DSS website, the System Security Plan (SSP) must (under the vulnerability reporting requirement of paragraph 8-610a(1)(c)) include a description of how and why the contractor has deviated from the standard, and a risk acceptance statement by the GCA.

Trusted Downloading Procedures do not need to be followed when classified information is transferred from an accredited PL 1 system storing the same level of classified information from multiple programs to media that will be handled and then remain at the same or higher level classified environment and controls (i.e., handling, marking, distribution/access controls, safeguarding, etc.). However, a review must be accomplished to ensure that only the designated files were transferred to the

new media. This could include a review of hard copy output and/or a visual review of the electronic file.

ISL 2007-01 #27 (8-305, 8-103.f.(5)). What are the NISPOM security requirements for protection against malicious code in IS?

Answer: NISPOM requires that all IS, regardless of the OS, are protected against malicious code. The ISSM must implement policies and procedures that detect and deter incidents caused by malicious code, viruses, intruders, or unauthorized modifications to software or hardware. The IS must employ the appropriate software to check all files for viruses and malicious code before being introduced on an IS.

8-306. Marking Hardware, Output, and Media. Markings on hardware, output, and media shall conform to Chapter 4 of this manual. If the required marking is impractical or interferes with the operation of the media, the CSA may approve alternate marking procedures.

a. **Hardware Components.** All components of an IS, including input/output devices that have the potential for retaining information, terminals, stand-alone microprocessors, or word processors used as terminals, shall bear a conspicuous, external label that states the highest classification level and most restrictive classification category of the information accessible to the component in the IS. This labeling may be accomplished using permanent markings on the component, a sign placed on the terminal, or labels generated by the IS and displayed on the screen. If the CSA requires that labels be color coded to indicate classification level they shall be orange for Top Secret, red for Secret, blue for Confidential, and green for unclassified.

ISL 2007-01 #28 (8-306.a.). Are external color-coded labels required per paragraph 8-306a?

Answer: No, the NISPOM does not require color-coded labels to indicate classification level.

b. **Hard Copy Output and Removable Media.** Hard copy output (paper, fiche, film, and other printed media) and removable media shall be marked with visible, human-readable, external markings to the accreditation level of the IS unless an appropriate classification review has been conducted or in the

case of media, the information has been generated by a tested program verified to produce consistent results and approved by the CSA. Such programs will be tested on a statistical basis to ensure continuing performance.

ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)c)). Can DSS provide additional guidance on the trusted download process and the requirement for output and media review?

Answer: Yes, Due to the diversity and uniqueness of the numerous vendor platforms and applications in use (e.g., word processing, database, electronic mail, and spreadsheets), a thorough review by the ISSM and DSS must be conducted before the trusted downloading procedures are used to create classified or unclassified electronic files and/or media.

All trusted downloading procedures must use new media. This mitigates the possibility of classified system contamination or corruption, as used media could contain and inadvertently introduce unauthorized software into the classified system.

The DSS Trusted Downloading Procedures can be found on the DSS web site (www.dss.mil) under the Industrial Security Program link. These procedures support many of the standard applications and can be used to examine information that is not in human readable form with the reasonable assurance that only the requested information was transferred.

If the ISSM is unable to implement the DSS procedures found on the DSS website, the System Security Plan (SSP) must (under the vulnerability reporting requirement of paragraph 8-610a(1)(c)) include a description of how and why the contractor has deviated from the standard, and a risk acceptance statement by the GCA.

Trusted Downloading Procedures do not need to be followed when classified information is transferred from an accredited PL 1 system storing the same level of classified information from multiple programs to media that will be handled and then remain at the same or higher level classified environment and controls (i.e., handling, marking, distribution/access controls, safeguarding, etc.). However, a review must be accomplished to ensure

that only the designated files were transferred to the new media. This could include a review of hard copy output and/or a visual review of the electronic file.

c. Unclassified Media. In the CSA-approved areas where classified and unclassified information are processed on collocated IS, unclassified media shall be so marked.

ISL 2007-01 #29 (8-306.c.). This paragraph requires that unclassified media be marked when classified and unclassified IS are collocated. Since the DSS approved area can range in size and structure (e.g., from a small office cubicle to a multi-story building) can DSS provide additional guidance?

Answer: Externally marking media when classified and unclassified IS are collocated clearly communicates and distinguishes the classification level of the media. The ISSM/ISSO must establish well-defined perimeters for the classified IS. These perimeters not only set apart the classified area, but assist in distinguishing classified media from unclassified media within the area. Writeable media within the classified IS area perimeter that is unmarked and not in factory-sealed packages must be considered classified, and must be marked and protected accordingly. Writeable media not in the classified IS area that is unmarked is considered unclassified unless circumstances dictate a conclusion that the material is in fact classified.

8-307. Personnel Security. Personnel with system access play an integral role in protecting information; defining their system security policies; and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their IS. Duties, responsibilities, privileges, and specific limitations of IS users, both general and privileged, shall be specified in writing. So far as feasible, security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the system. Protection levels for particular IS shall be determined by the clearance level, formal access approvals, and need-to-know held by users of the IS, and the classification level of data processed or stored.

8-308. Physical Security

a. Safeguards shall be established that prevent or detect unauthorized access to the IS and unauthorized modification of the IS hardware and software. Hardware integrity of the IS, including remote equipment, shall be maintained at all times, even when all classified information has been removed from the IS.

ISL 2007-01 #30 (8-308.a.). How is hardware integrity of an IS maintained?

Answer: Hardware integrity can be maintained by one or more of the following methods:

a) Continuous supervision by authorized personnel.

b) Use of approved cabinets, enclosures, seals, locks or closed areas.

c) Use of area controls that prevent or detect tampering of the IS hardware and/or software. These controls will vary depending on the security in-depth at the contractor's facility and in the immediate area of the IS.

b. Classified processing shall take place in a CSA-approved area.

ISL 2007-01 #31 (8-308.b.). What is the boundary of the DSS approved area for classified processing?

Answer: The physical boundary of the DSS approved area for classified processing is limited to the area within which authorized contractor personnel can exercise constant surveillance and maintain control of the IS. The area must have an identifiable boundary (e.g., walls, signs, tape on floor, rope or chains, etc.) where it is obvious that the area is restricted to only authorized personnel. Unattended classified processing requires a closed area and supplemental controls depending upon the accreditation level of the IS.

c. Visual Access. Devices that display or output information in human-readable form shall be positioned to prevent unauthorized individuals from reading the information.

d. Unescorted Access. All personnel granted unescorted access to the area containing the IS shall have an appropriate security clearance.

8-309. Protection of Media. Media must be protected to the level of accreditation until an appropriate classification review has been conducted.

ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)(c)). Can DSS provide additional guidance on the trusted download process and the requirement for output and media review?

Answer: Yes, Due to the diversity and uniqueness of the numerous vendor platforms and applications in use (e.g., word processing, database, electronic mail, and spreadsheets), a thorough review by the ISSM and DSS must be conducted before the trusted downloading procedures are used to create classified or unclassified electronic files and/or media.

All trusted downloading procedures must use new media. This mitigates the possibility of classified system contamination or corruption, as used media could contain and inadvertently introduce unauthorized software into the classified system.

The DSS Trusted Downloading Procedures can be found on the DSS web site (www.dss.mil) under the Industrial Security Program link. These procedures support many of the standard applications and can be used to examine information that is not in human readable form with the reasonable assurance that only the requested information was transferred.

If the ISSM is unable to implement the DSS procedures found on the DSS website, the System Security Plan (SSP) must (under the vulnerability reporting requirement of paragraph 8-610a(1)(c)) include a description of how and why the contractor has deviated from the standard, and a risk acceptance statement by the GCA.

Trusted Downloading Procedures do not need to be followed when classified information is transferred from an accredited PL 1 system storing the same level of classified information from multiple programs to media that will be handled and then remain at the same or higher level classified environment and controls (i.e., handling, marking,

distribution/access controls, safeguarding, etc.). However, a review must be accomplished to ensure that only the designated files were transferred to the new media. This could include a review of hard copy output and/or a visual review of the electronic file.

8-310. Review of Output and Media

a. **Human-Readable Output Review.** An appropriate sensitivity and classification review shall be performed on human-readable output before the output is released outside the security boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.

ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)(c)). Can DSS provide additional guidance on the trusted download process and the requirement for output and media review?

Answer: Yes, Due to the diversity and uniqueness of the numerous vendor platforms and applications in use (e.g., word processing, database, electronic mail, and spreadsheets), a thorough review by the ISSM and DSS must be conducted before the trusted downloading procedures are used to create classified or unclassified electronic files and/or media.

All trusted downloading procedures must use new media. This mitigates the possibility of classified system contamination or corruption, as used media could contain and inadvertently introduce unauthorized software into the classified system.

The DSS Trusted Downloading Procedures can be found on the DSS web site (www.dss.mil) under the Industrial Security Program link. These procedures support many of the standard applications and can be used to examine information that is not in human readable form with the reasonable assurance that only the requested information was transferred.

If the ISSM is unable to implement the DSS procedures found on the DSS website, the System Security Plan (SSP) must (under the vulnerability reporting requirement of paragraph 8-610a(1)(c)) include a description of how and why the contractor has deviated from the standard, and a risk acceptance statement by the GCA.

Trusted Downloading Procedures do not need to be followed when classified information is transferred from an accredited PL 1 system storing the same level of classified information from multiple programs to media that will be handled and then remain at the same or higher level classified environment and controls (i.e., handling, marking, distribution/access controls, safeguarding, etc.). However, a review must be accomplished to ensure that only the designated files were transferred to the new media. This could include a review of hard copy output and/or a visual review of the electronic file.

b. **Media Review.** Electronic output, such as files, to be released outside the security boundary shall be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content using the appropriate software application. CSA-approved random or representative sampling techniques may be used to verify the proper marking of large volumes of output.

8-311. Configuration Management. Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.

ISL 2007-01 #32 (8-311). Do operating system (OS) and application software need to be updated?

Answer: Yes. Patch management (e.g., installation of system software updates) is an important aspect of configuration management, which is in turn crucial in preventing malicious code from infecting an IS and its data.

a. **Configuration Documentation.** Procedures shall be implemented to identify and document the type, model, and brand of system or network component (e.g., a workstation, personal computer, or router), security-relevant software product names

and version or release numbers, and physical location.

b. **System Connectivity.** Procedures shall be implemented to identify and document system connectivity, including any software used for wireless communication, and any communications media.

c. **Connection Sensitivity.** The sensitivity level of each connection or port controlled by the Security Support Structure (SSS) shall be documented.

d. **CM Plan.** The facility CM program shall be documented in a CM plan and shall include:

(1) Formal change control procedures to ensure the review and approval of security-relevant hardware and software.

(2) Procedures for management of all documentation, such as the SSP and security test plans, used to ensure system security.

(3) Workable processes to implement, periodically test, and verify the CM plan.

(4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.

Section 4. Protection Measures

8-400. Protection Profiles. Protection profiles required for a particular IS are determined by the Level of Concern for Confidentiality and by the operating environment of the system as reflected by the clearances, access approvals and need-to-know embodied in the user environment. Operational data integrity and system availability, while important security concerns, are not covered by the NISP and will be determined in additional guidance or requirements issued by the GCA. However, provisions for integrity and availability concerns are included in this Chapter to provide guidance when the GCA contractually imposes them.

ISL 2007-01 #2 (8-100.a., 8-400). NISPOM Paragraph 8-100a states that the IS must be properly managed to protect against loss of data integrity and to ensure the availability of the data and system. Is paragraph 8-100.a. a statement of general security concerns or is it a National Industrial Security Program Operating Manual (NISPOM) requirement?

Answer: Paragraph 8-100.a. states a baseline standard. As stated in paragraph 8-400, the Government Contracting Activity (GCA)) will issue additional guidance or requirements if there is a need for data integrity and system availability controls.

ISL 2007-01 #33 (8-400, 8-100.c.). NISPOM Paragraph 8-100c states that "additional requirements for high-risk systems and data are covered in the NISPOM Supplement." What is the definition of "high-risk" systems and data? What are the security requirements for contractors who need to develop systems at PL 4?

Answer: A high-risk system is one that requires protection above the NISPOM baseline (i.e., multi-level) where high-risk data would be Special Access Program (SAP) or Special Compartment Information (SCI) information. Standards for SAP and SCI are typically established in contract documents by the responsible GCA.

8-401. Level of Concern. The level of concern reflects the sensitivity of the information and the consequences of the loss of confidentiality, integrity or availability.

ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)(c)). Can DSS provide additional guidance on the trusted download process and the requirement for output and media review?

Answer: Yes, Due to the diversity and uniqueness of the numerous vendor platforms and applications in use (e.g., word processing, database, electronic mail, and spreadsheets), a thorough review by the ISSM and DSS must be conducted before the trusted downloading procedures are used to create classified or unclassified electronic files and/or media.

All trusted downloading procedures must use new media. This mitigates the possibility of classified system contamination or corruption, as used media could contain and inadvertently introduce unauthorized software into the classified system.

The DSS Trusted Downloading Procedures can be found on the DSS web site (www.dss.mil) under the Industrial Security Program link. These procedures support many of the standard applications and can be used to examine information that is not in human readable form with the reasonable assurance that only the requested information was transferred.

If the ISSM is unable to implement the DSS procedures found on the DSS website, the System Security Plan (SSP) must (under the vulnerability reporting requirement of paragraph 8-610a(1)(c)) include a description of how and why the contractor has deviated from the standard, and a risk acceptance statement by the GCA.

Trusted Downloading Procedures do not need to be followed when classified information is transferred from an accredited PL 1 system storing the same level of classified information from multiple programs to media that will be handled and then remain at the same or higher level classified environment and controls (i.e., handling, marking, distribution/access controls, safeguarding, etc.). However, a review must be accomplished to ensure that only the designated files were transferred to the new media. This could include a review of hard copy output and/or a visual review of the electronic file.

a. **Information Sensitivity Matrices.** The matrices presented in Tables 1, 2, and 3 are designed to assist the CSA, with input from the ISSM in determining the appropriate protection level for confidentiality, and the level of concern for integrity, and availability, if contractually mandated, for a given IS processing a given set of information. The Information Sensitivity Matrices should be used as follows:

(1) A determination of high, medium, or basic shall be made for each of the three attributes: confidentiality, integrity, and availability. It is not necessary for the level of concern to be the same for all attributes of the system.

(2) When multiple applications on a system result in different levels of concern for the categories of confidentiality, integrity and availability the highest level of concern for each category shall be used.

b. **Confidentiality Level of Concern.** In considering confidentiality, the principal question is the necessity for supporting the classification levels and the categories of information (e.g., Secret National Security Information) on the system in question. The Protection Level Table for Confidentiality (Table 4) combines the processing environment with the level of concern for confidentiality to provide a Protection Level. The Protection Level is then applied to Table 5 to provide a set of graded requirements to protect the confidentiality of the information on the system.

c. **Integrity Level of Concern.** In considering integrity, the principal question is the necessity for maintaining the integrity of the information on the system in question.

d. **Availability Level of Concern.** In considering availability, the principal consideration is the need for the information on the system in question to be available in a fixed time frame to accomplish a mission.

8-402. Protection Level. The protection level of an IS is determined by the relationship between two parameters: first, the clearance levels, formal access approvals, and need-to-know of users; and second, the level of concern based on the classification of the

data on a particular system. The protection level translates into a set of requirements (tables 5, 6, and 7) that must be implemented in the resulting system. Table 4 presents the criteria for determining the following three protection levels for confidentiality.

a. Systems are operating at Protection Level 1 when all users have all required approvals for access to all information on the system. This means that all users have all required clearances, formal access approvals, and the need-to-know for all information on the IS, i.e. dedicated mode.

b. Systems are operating at Protection Level 2 when all users have all required clearances, and all required formal access approvals, but at least one user lacks the need-to-know for some of the information on the system, i.e. a system high mode.

c. Systems are operating at Protection Level 3 when all users have all required clearances, but at least one user lacks formal access approval for some of the information on the system, i.e. compartmented mode.

8-403. Protection Profiles. Protection requirements graded by levels of concern and confidentiality protection level are detailed in Section 6. Tables 5, 6, and 7 present the requirements detailed in Section 6. To use these tables, find the column representing the protection level for confidentiality, or, if contractually mandated, find the column representing the level of concern for integrity or availability.

a. **Confidentiality Components.** Confidentiality components describe the confidentiality protection requirements that must be implemented in an IS using the profile. The confidentiality protection requirements are graded according to the confidentiality protection levels.

b. **Integrity Components.** Integrity components, if applicable, describe the integrity protection requirements that must be implemented in an IS using the profile. The integrity protection requirements are graded according to the integrity level of concern.

c. **Availability Components.** Availability components, if applicable, describe the availability protection requirements that must be implemented in

an IS using the profile. The availability protection requirements are graded according to the availability level of concern.

Table 1. Information Sensitivity Matrix for Confidentiality

Level of Concern	Qualifiers
High	TOP SECRET and SECRET Restricted Data (SIGMAs 1,2,14,15)
Medium	SECRET SECRET Restricted Data
Basic	CONFIDENTIAL

Table 2. Information Sensitivity Matrix for Integrity

Level of Concern	Qualifiers
High	Absolute accuracy required for mission accomplishment; or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests; or loss of integrity will have an adverse effect on confidentiality.
Medium	High degree of accuracy required for mission accomplishment, but not absolute; or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organizational-level interests.
Basic	Reasonable degree of accuracy required for mission accomplishment.

Table 3. Information Sensitivity Matrix for Availability

Level of Concern	Qualifiers
High	Information must always be available upon request, with no tolerance for delay; or loss of life might result from loss of availability; or loss of availability will have an adverse effect on national-level interests; or loss of availability will have an adverse effect on confidentiality.
Medium	Information must be readily available with minimum tolerance for delay; or bodily injury might result from loss of availability; or loss of availability will have an adverse effect on organizational-level interests.
Basic	Information must be available with flexible tolerance for delay.

NOTE: In this context, “High - no tolerance for delay” means no delay; “Medium - minimum tolerance for delay” means a delay of seconds to hours; and “Basic - flexible tolerance for delay” means a delay of days to weeks. In the context of the NISPOM, integrity and availability shall only apply when they have a direct impact on protection measures for confidentiality, i.e., integrity of the password file, integrity of audit logs or when contractually imposed.

Table 4. Protection Level Table for Confidentiality

Level of Concern	Lowest Clearance	Formal Access Approval	Need-To-Know	Protection Level
High, Medium, or Basic	At Least Equal to Highest Data	NOT ALL Users Have ALL	Not contributing to the decision	3
High, Medium, or Basic	At Least Equal to Highest Data	ALL Users Have ALL	NOT ALL Users Have ALL	2
High, Medium, or Basic	At Least Equal to Highest Data	ALL Users Have ALL	ALL Users Have ALL	1

Table 5. Protection Profile Table for Confidentiality

Requirements (Paragraph)	Confidentiality Protection Level		
	P L 1	PL 2	PL 3
Audit Capability (8-602)	Audit 1	Audit 2	Audit 3 Audit 4
Data Transmission (8-605)	Trans 1	Trans 1	Trans 1
Access Controls (8-606)	Access 1	Access 2	Access 3
Identification & Authentication (8-607)	I&A 1	I&A 2,3,4	I&A2,4,5
Resource Control (8-608)		ResrcCtrl 1	ResrcCtrl 1
Session Controls (8-609)	SessCtrl 1	SessCtrl 2	SessCtrl 2
Security Documentation (8-610)	Doc 1	Doc 1	Doc 1
Separation of Functions (8-611)			Separation
System Recovery (8-612)	SR 1	SR 1	SR 1
System Assurance (8-613)	SysAssur 1	SysAssur 1	SysAssur 2
Security Testing (8-614)	Test 1	Test 2	Test 3

Table 6. Protection Profile Table for Integrity

Requirements (Paragraph)	Integrity Level of Concern		
	Basic	Medium	High
Audit Capability (8-602)	Audit 1	Audit 2	Audit 3
Backup and Restoration of Data (8-603)	Backup 1	Backup 2	Backup 3
Changes to Data (8-604)		Integrity 1	Integrity 2
System Assurance (8-613)		SysAssur 1	SysAssur 2
Security Testing (8-614)	Test 1	Test 2	Test 3

Table 7. Protection Profile Table for Availability

Requirements (Paragraph)	Availability Level of Concern		
	Basic	Medium	High
Alternate Power Source (8-601)		Power 1	Power 2
Backup and Restoration of Data (8-603)	Backup 1	Backup 2	Backup

Section 5. Special Categories

8-500. Special Categories. Several categories of systems can be adequately secured without implementation of all the technical features specified this Chapter. These systems are not “exceptions” or “special cases” but applying the technical security requirements to these systems by rote results in unnecessary costs and operational impacts. In general, the technical questions are where, when, and how to apply a given set of protection measures, rather than whether to apply the measures. For many of these “special” systems (such as guards or pure servers; and tactical, embedded, data-acquisition, and special-purpose systems), the physical security protections for the system provide the required access control, while the application running on the platform provides the required user separation.

ISL 2007-01 #34 (8-500, 8-503.b.). Why are the Chapter 8 technical security requirements different for the platforms of Special Category systems (such as guards and servers) than for applications of the Special Category guards or servers?

Answer: Special category systems do not require all the technical features and safeguards of Chapter 8 to be adequately secured. The application running on a guard or server is viewed separately from the hardware and OS platform. The platform of the guard or pure server may be at a PL lower than the PL associated with the application(s) due to its large number of users. The guard or pure server application itself must provide the more stringent technical protections appropriate to the systems’ PL and operational environment.

ISL 2007-01 #41 (8-602, 8-500). If an IS is capable of auditing, must the contractor enable this feature?

Answer. Yes. The contractors must make every effort to meet NISPOM Chapter 8 auditing requirements, to include upgrading their operating system as appropriate and/or obtaining third party software, if necessary. However, an exception to this requirement may be invoked in situations where a GCA certifies one or more of the following:

a) The contractor is required to use an OS that is not capable of meeting Chapter 8 audit requirements;

b) Enabling auditing on a legacy OS will result in unnecessary costs, operational impacts, or deviation from the secure deployed operating environment; or,

c) The IS is a Special Category System, meets NISPOM 8-500 requirements and can be adequately secured without all Chapter 8 technical requirements being implemented.

In these three instances, a NISPOM waiver is not required. Contract documentation from the GCA, such as the DD Form 254, formal classification guidance and/or a formal memorandum that clearly cites one or more of the circumstances cited above must be provided to DSS. A suggested format is a statement such as, “the contractor is required to use Windows 98,” followed by the rationale for its use. The statement must be signed by the Contracting Officer, the Contracting Officer’s Representative (COR) or the Contracting Officer’s Technical Representative (COTR), or the Government Program Manager. A formal contract modification is not necessary.

8-501. Single-user, Stand-alone Systems. Extensive technical protection measures are normally inappropriate and inordinately expensive for single-user, stand-alone systems. The CSA can approve administrative and environmental protection measures for such systems, in lieu of technical ones. Systems that have one user at a time, but have a total of more than one user with no sanitization between users, are multi-user systems, and the CSA shall consider the systems as such in determining the protection level and the resulting security requirements. Systems that have one user at a time, are sanitized between users and periods of different classification/sensitivity, are periods processing systems as described below.

ISL 2007-01 #16 (8-301.a., 8-501). Can DSS provide more guidance on when sanitization or clearing of memory and media is required?

Answer: Sanitization of memory and media is required when the memory or media is no longer needed to store classified information. Clearing is required before and after periods of processing as a method of ensuring need-to-know protection, and prior to maintenance. Clearing is all that is required when the memory or media will be used at a higher classification level or at a more restrictive information sensitivity level. The clearing and sanitization matrix is available on the DSS web site. Users unable to access the matrix should contact their local DSS Industrial Security Representative.

ISL 2007-01 #35 (8-501). Can an IS that is used by more than one person be considered a single user standalone IS?

Answer: A single user standalone IS is defined as an IS physically and electronically isolated from all other systems and is intended for use by one person only, e.g., a laptop assigned to one person, a personal computer assigned to one individual. An IS with more than one user will be considered a single user standalone if each user of the IS has an individually assigned removable hard drive and the system is sanitized between users. Information Technology support personnel are not considered users of single user standalone systems.

8-502. Periods Processing. Periods processing is a method of sequential operation of an IS that provides the capability to process information at various levels of sensitivity at distinctly different times.

ISL 2007-01 #36 (8-502). Can an IS being upgraded to process classified information be booted from a floppy disk or CD-ROM?

Answer: Yes, provided the floppy disk or CD ROM is protected to the level of the IS and is used in a read-only configuration. However, DSS recommends that classified IS be configured to boot only from specific hard drives to minimize the possibility of security controls being circumvented by external media.

a. Periods processing provides the capability to either have more than one user or group of users (sequentially) on a single-user IS who do not have the same need-to-know or who are authorized to access

different levels of information; or use an IS at more than one protection level (sequentially).

b. Sanitization After Use. If an IS is used for periods processing either by more than one user or for segregating information by classification level onto separate media, the SSP shall specify the sanitization procedures to be employed by each user before and after each use of the system.

c. Sanitization Between Periods. The IS shall be sanitized of all information before transitioning from one period to the next (e.g., whenever there will be a new user(s) who does not have an access authorization or need-to-know for data processed during the previous period, changing from one protection level to another). These procedures shall be documented in the SSP. Such procedures could include, among others, sanitizing non-volatile storage, exchanging disks, and powering down the IS and its peripherals.

d. Media For Each Period. An IS employed in periods processing shall have separate media for each period of processing, including copies of operating systems, utilities, and applications software.

e. Audit. If there are multiple users of the system and the system is not capable of automated logging, the CSA shall consider requiring manual logging. Audit trails are not required for single-user stand-alone systems.

ISL 2007-01 #37 (8-502.e). Paragraph 8-502.e. states that the CSA shall consider manual logging for multiple user systems that are not capable of automated logging. Does the NISPOM require manual logging, and if so, can access lists be used for validation purposes?

Answer: As provided for in 8-502e, DSS requires manual logging when automated logging cannot be accomplished. DSS can approve alternate procedures for accountability of user activities on an IS that mitigate risk to an acceptable level. Manual logs and access control lists (i.e., physical assess) can be used for validation purposes and shall be retained as an Audit 1 requirement.

8-503. Pure Servers

a. Certain specialized systems, when acting as pure servers in a network, do not fit the protection level criteria and may need fewer technical security countermeasures. These systems have the following characteristics:

- (1) No user code is present on the system.
- (2) Only system administrators and maintainers can access the system.
- (3) The system provides non-interactive services to clients (e.g., packet routing or messaging services).
- (4) The hardware and/or application providing network services otherwise meet the security requirements of the network.
- (5) The risk of attack against the Security Support Structure (SSS) using network communication paths is sufficiently low.
- (6) The risk of attack against the SSS using physical access to the system itself is sufficiently low.

b. The platform (i.e., hardware and operating system) on which the guard or pure server runs usually needs to meet no more than Protection Level 3 security requirements. The guard or pure server may have a large number of clients (i.e., individuals who use the guard or server functional capabilities in a severely constrained way). The guard application or server application itself will have to provide the more stringent technical protections appropriate for the system's protection level and operational environment. Assurances appropriate to the levels of concern for the system shall be implemented.

ISL 2007-01 #34 (8-500, 8-503.b.). Why are the Chapter 8 technical security requirements different for the platforms of Special Category systems (such as guards and servers) than for applications of the Special Category guards or servers?

Answer: Special category systems do not require all the technical features and safeguards of Chapter 8 to

be adequately secured. The application running on a guard or server is viewed separately from the hardware and OS platform. The platform of the guard or pure server may be at a PL lower than the PL associated with the application(s) due to its large number of users. The guard or pure server application itself must provide the more stringent technical protections appropriate to the systems' PL and operational environment.

ISL 2007-01 #38 (8-503.b.). Paragraph 8-503.b. states that the platform on which the guard or server runs usually needs to meet no more than Protection Level (PL) 3 security requirements. Is this correct since Chapter 8 only has 3 PLs?

Answer: Yes, the platform on which the guard or server runs usually must meet no more than PL 3 requirements, given that PL3 represents the most stringent protection requirements identified in Chapter 8. However, a higher PL specified in a more stringent standard (e.g., DCID 6-3) may be imposed by contract. Table 5, Protection Profile for Confidentiality (NISPOM Chapter 8, Section 4) illustrates a matrix of eleven (11) graded protection requirements for the three (3) PLs. The platform's set of graded protection requirements will depend on the confidentiality PL and the level of concern (high, medium, and basic) for the data being processed or stored. The platform is not restricted to a single PL for all 11 requirements; for example, the platform may have an access requirement of PL3 but an auditing requirement of PL1.

ISL 2007-01 #39 (8-503.b.). Do "pure servers" (e.g., guard, proxy server, application server) require accreditation separate from the general-purpose computers they support or are connected to?

Answer: Normally the only "pure server" that requires separate accreditation is a guard. The guard requires more stringent technical protection and assurance than the IS it protects by the very nature of its function. The other types of "pure servers" can be described and included in the general-purpose computer SSP.

c. Systems that have general users or execute general user code are not "pure servers" within the meaning of this section, and so must meet all security

requirements specified for their protection level and operational environment.

d. The term “pure server” is not intended to limit the applicability of this section to systems that have traditionally been referred to as servers. For example, a messaging system that happened to be implemented on a general-purpose computer platform could be accredited under this section and, if such a system meets the specifications in a, above, the system’s technical requirements could be categorized by this section.

e. The above easing of technical security requirements does not imply any relaxation in other security requirements (e.g., physical and communications security requirements) which are determined by the information handled or protected by the system. As stated above, this easing of technical requirements is predicated upon adequate application of physical security and other appropriate security disciplines.

8-504. Tactical, Embedded, Data-Acquisition, and Special-Purpose Systems. Some systems are incapable of alteration by users and are designed and implemented to provide a very limited set of predetermined functions. Certain tactical or so-called “embedded” systems fall into this category, as do some data-acquisition systems and some other special-purpose systems. These systems also have the characteristics that: first and most importantly, there are no general users on the system; and, second, there is no user code running on the system. If the CSA determines that such a system is sufficiently incapable of alteration, and that the application(s) running on the system provide an adequate level of security, then the system does not have to meet additional security requirements specified for more-general-purpose systems in this section. The CSA and implementers are cautioned to be sure that such systems do, in all operational situations, provide the separation appropriate to the system’s protection level.

ISL 2007-01 #40 (8-504). What security requirements apply to systems that are tactical and/or embedded as an integral element of a larger system?

Answer. DSS has been receiving questions as to what security requirements apply to systems that are

embedded as an integral element of a larger system (NISPOM 8-504). The following guidance is provided:

While certain types and configurations of equipment or components fit the definition of an information system₁ (IS) requiring accreditation, others may not. The Information System Security Manager (ISSM) will determine and document the capabilities of such equipment to collect and process classified information. As a general rule, equipment composed of volatile memory with no other storage media (such as test equipment) does not require accreditation.

Security requirements for information systems that are embedded as an integral element of a larger system that is used to perform or control a specific function (such as control systems or weapons systems) should be established by the Government Contracting Activity (GCA) concurrently with the design and development of the system. If the GCA has not provided those requirements, the contractor shall request them from the GCA. Regardless of the existence of guidance from the GCA, these systems will not require Cognizant Security Agency (CSA) accreditation. However, if GCA security requirements are not provided, the contractor will be required to submit classified processing procedures to the CSA that describe the security requirements and procedures implemented that protect the embedded system and classified information against unauthorized disclosure or loss.

8-505. Systems with Group Authenticators. Many security measures specified in this section implicitly assume that the system includes an acceptable level of individual accountability. This is normally ensured by the use of unique user identifiers and authenticators. Operationally, the design of some systems necessitates more than one individual using the same identifier/ authenticator combination. Such situations are often referred to as requiring the use of group authenticators. In general, the use of group authenticators precludes the association of a particular act with the individual who initiated that act. In turn, this can preclude assignment of responsibility and can exacerbate the difficulties involved in incident investigation. Group authenticators shall be used only for broader access after the use of a unique authenticator for initial identification and authentication, and documented in

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

SSP. Group authenticators may not be shared with anyone outside of the group.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 6. Protection Requirements

ISL 2009-01 (8-101.a., 8-202, Chapter 8 Section 6). This Industrial Security Letter (ISL) pertains to the DSS ODAA “Standardization of Baseline Technical Security Configurations,” hereafter referred to as the “Baseline Standards.”

In accordance with its National Industrial Security Program oversight responsibilities, and as provided for in NISPOM 8-202, DSS has established an approved set of technical safeguards that DSS will apply in making a decision to accredit an IS. These technical safeguards are set forth in the Baseline Standards. The technical configurations prescribed in the Baseline Standards conform to NISPOM protection requirements (Section 6 of Chapter 8), as well as to Federal standards that apply to Government systems.

Using the baseline set of safeguards in the Baseline Standards will assist contractors in meeting their requirement to select, test, certify and document that a baseline of technical security controls has been implemented.

Contractor application of the safeguards in the Baseline Standards will facilitate the DSS decision to accredit an IS; that is, for DSS to take a risk-management approach to authorize an IS to operate in accordance with a specific set of baseline security settings for a specific IS in a specific environment and explicitly accepting the residual risk.

The Baseline Standards is available on the DSS website: www.dss.mil.

8-600. Introduction. This section describes the implementation requirements for different protection measure.

8-601. Alternate Power Source (Power). An alternate power source ensures that the system availability is maintained in the event of a loss of primary power. An APS can also provide a time period for orderly system shutdown or the transfer of system operations to another system or power source.

a. **Power 1 Requirements.** Procedures for the graceful shutdown of the system shall ensure no loss of data. The decision not to use an alternate source

of power, such as an uninterruptible power supply (UPS) for the system, shall be documented.

b. **Power 2 Requirements.** Instead of Power 1, procedures for transfer of the system to another power source shall ensure that the transfer is completed within the time requirements of the application(s) on the system.

8-602. Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.

ISL 2007-01 #41 (8-602, 8-500). If an IS is capable of auditing, must the contractor enable this feature?

Answer. Yes. The contractors must make every effort to meet NISPOM Chapter 8 auditing requirements, to include upgrading their operating system as appropriate and/or obtaining third party software, if necessary. However, an exception to this requirement may be invoked in situations where a GCA certifies one or more of the following:

a) The contractor is required to use an OS that is not capable of meeting Chapter 8 audit requirements;

b) Enabling auditing on a legacy OS will result in unnecessary costs, operational impacts, or deviation from the secure deployed operating environment; or,

c) The IS is a Special Category System, meets NISPOM 8-500 requirements and can be adequately secured without all Chapter 8 technical requirements being implemented.

In these three instances, a NISPOM waiver is not required. Contract documentation from the GCA, such as the DD Form 254, formal classification guidance and/or a formal memorandum that clearly cites one or more of the circumstances cited above must be provided to DSS. A suggested format is a statement such as, “the contractor is required to use Windows 98,” followed by the rationale for its use.

The statement must be signed by the Contracting Officer, the Contracting Officer's Representative (COR) or the Contracting Officer's Technical Representative (COTR), or the Government Program Manager. A formal contract modification is not necessary.

ISL 2007-01 #42 (8-602). What security relevant activities should be recorded for all PLs and all Special Category IS?

Answer: Security relevant activities are those identified in Paragraph 8-602 audit requirements 1-4 that identify IS security relevant activities normally captured by an automated audit capability for all PLs and those Special Category Systems that have the capability to do so without adverse impact on operations. Additionally, manual logs are required for:

a) Maintenance, repair, installation, or removal of hardware components. Log must include the component involved, the action taken and the name of the escort if the maintenance was performed by an un-cleared individual.

b) Installation, testing, and modification of operating system and security-related software (if applicable). Logs must identify the software involved.

c) Periods processing times.

d) Sanitization and declassifying memory, media and devices.

e) Application and reapplication of security seals (if applicable).

ISL 2007-01 #43 (8-602). How long should audit records be retained?

Answer: Audit records must be retained covering the previous 12 months.

a. Audit 1 Requirements

ISL 2007-01 #44 (8-602.a). Can DSS provide clarification on the NISPOM Paragraph 8-602 auditing requirements for Security Relevant Object (SRO)?

Answer. The following chart identifies auditing requirements by type of Security Relevant Object (SRO), protection level and whether the attempt to access the SRO was successful or not. For example, only unsuccessful attempts to access operating system executables are required to be audited at the PL-1 level. Auditing scripts and a list of security relevant objects for use by contractors are on the DSS web site (www.dss.mil) under "ODAA Tools".

Security Relevant Object (SRO)	PL-1	PL-2	PL-3	PL-4 NISPOMSUP
Operating system executables	U	U	S, U	S, U
Operating system configuration	U	U	S, U	S, U
System management and maintenance executables	U	U	S, U	S, U
Audit data	U	U	S, U	S, U
Security related software	U	U	S, U	S, U
User files, classified data	(no auditing)	U	S, U	S, U

S-Successful

U-Unsuccessful

(1) Automated Audit Trail Creation: The system shall automatically create and maintain an audit trail or log (On a PL-1 system only: In the event that the Operating System cannot provide an automated audit capability, an alternative method of accountability for user activities on the system shall be developed and documented.) Audit records shall be created to record the following:

(a) Enough information to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.

(b) Successful and unsuccessful logons and logoffs.

(c) Successful and unsuccessful accesses to security-relevant objects and directories, including creation, open, close, modification, and deletion.

ISL 2007-01 #45 (8-602.a.(1)(c)). This paragraph requires the auditing of security relevant objects (SRO) and directories. Can DSS provide clarification on OS configuration and location of SRO?

Answer. All OS contain SRO and directories but the location (folder or directory) and the OS configuration may vary with the OS. The following table represents a standard configuration of SRO to be audited for Windows NT and UNIX. Please note that while the SRO and directories will remain constant, directory examples can vary by installation, by administrator and by OS.

Security Relevant Objects (SRO)	Directory Examples (can vary by installation)	
	Windows	Unix
Operating system executables	Refer to the Security Relevant Objects list located under "ODAA Tools" on the DSS web site (www.dss.mil).	/bin and /usr/bin
Operating system configuration		/etc
System management and maintenance executables		/etc, /sbin, /usr/sbin
Audit data	C:\WINNT\system32\config	/var/audit
Security related software	C:\Program files\NispUtilities	/usr/local or /opt
User files/classified data beginning at PL-2	C:\Profiles or C:\Documents and Settings	/home

(d) Changes in user authenticators.

(e) The blocking or blacklisting of a user ID, terminal, or access port and the reason for the action.

(f) Denial of access resulting from an excessive number of unsuccessful logon attempts.

(2) Audit Trail Protection. The contents of audit trails shall be protected against unauthorized access, modification, or deletion.

(3) Audit Trail Analysis. Audit analysis and reporting shall be scheduled, and performed. Security relevant events shall be documented and reported. The frequency of the review shall be at least weekly and shall be documented in the SSP.

(4) Audit Record Retention. Audit records shall be retained for at least one review cycle or as required by the CSA.

b. Audit 2 Requirements. In addition to Audit 1:

(1) Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that

individual). Periodic testing by the ISSO or ISSM of the security posture of the IS.

c. Audit 3 Requirements. In addition to Audit 2:

(1) Automated Audit Analysis. Audit analysis and reporting using automated tools shall be scheduled and performed.

d. Audit 4 Requirements. In addition to Audit 3:

(1) An audit trail, created and maintained by the IS, that is capable of recording changes to mechanism's list of user formal access permissions.

8-603. Backup and Restoration of Data (Backup). The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.

a. Backup 1 Requirements

(1) Backup Procedures. Procedures for the regular backup of all essential and security-relevant

information, including software tables and settings, such as router tables, software, and documentation, shall be documented.

(2) Backup Frequency. The frequency of backups shall be defined by the ISSM, with the assistance of the GCA, and documented in the backup procedures.

b. **Backup 2 Requirements.** In addition to Backup 1:

(1). Backup Media Storage. Media containing backup files and backup documentation shall be stored at another location, such as another part of the same building, a nearby building, or off facility, so as to reduce the possibility that a common occurrence could eliminate the on-facility backup data and the off-facility backup data.

(2) Verification of Backup Procedures. Backup procedures shall be periodically verified.

c. **Backup 3 Requirements.** In addition to Backup 2:

(1) Information Restoration Testing. Incremental and complete restoration of information from backup media shall be tested on an annual basis.

8-604. Changes to Data (Integrity). The control of changes to data includes deterring, detecting, and reporting of successful and unsuccessful attempts to change data. Control of changes to data may range from simply detecting a change attempt to the ability to ensure that only authorized changes are allowed.

a. **Integrity 1 Requirements**

(1) Change Procedures. Procedures and technical system features shall be implemented to ensure that changes to the data and IS software are executed only by authorized personnel or processes.

b. **Integrity 2 Requirements.** In addition to Integrity 1:

(1) Transaction Log. A transaction log, protected from unauthorized changes, shall be available to allow the immediate correction of

unauthorized data and IS software changes and the off-line verification of all changes at all times.

8-605. Data Transmission (Trans). Information protection is required whenever classified information is to be transmitted through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).

a. **Trans 1 Requirements**

(1) Protections. One or more of the following protections shall be used.

(a) Information distributed only within an area approved for open storage of the information.

(b) NSA-approved encryption mechanisms appropriate for the encryption of classified information.

(c) Protected Distribution System.

8-606. Access Controls (Access). The IS shall store and preserve the integrity of the sensitivity of all information internal to the IS.

a. **Access 1 Requirements**

(1) Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

b. **Access 2 Requirements.** In addition to Access 1:

(1) Discretionary access controls shall be provided. A system has implemented discretionary access controls when the security support structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The discretionary access control policy includes administrative procedures to support the policy and its mechanisms.

c. **Access 3 Requirements.** In addition to Access 2:

(1) Some process or mechanism that allows users (or processes acting on their behalf) to determine the formal access approvals granted to another user.

(2) Some process or mechanism that allows users (or processes acting on their behalf) to determine the sensitivity level of data.

8-607. Identification and Authentication (I&A)

a. **I&A 1 Requirements.** Procedures that include provisions for uniquely identifying and authenticating the users. Procedures can be external to the IS (e.g., procedural or physical controls) or internal to the IS (i.e., technical). Electronic means shall be employed where technically feasible.

b. **I&A 2 Requirements.** In addition to I&A 1:

(1) An I&A management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified in the SSP:

(a) Initial authenticator content and administrative procedures for initial authenticator distribution.

(b) Individual and Group Authenticators. Group authenticators may only be used in conjunction with an individual/unique authenticator, that is, individuals must be authenticated with an individual authenticator prior to use of a group authenticator.

(c) Length, composition and generation of authenticators.

(d) Change processes (periodic and in case of compromise).

(e) Aging of static authenticators (i.e., not one-time passwords or biometric patterns).

(f) History of authenticator changes, with assurance of non-replication of individual authenticators.

ISL 2007-01 #46 (8-607.b.(f)). This paragraph requires that the IS be able to maintain a history of authenticator changes (e.g., password) with assurance of non-replication under the Audit 2 requirement. What does the contractor do if the IS is unable to meet this requirement?

Answer: The ISSM must document this as a unique vulnerability and describe compensating measures in the applicable SSP as required by paragraph 8- 610a (1).

(g) Protection of authenticators.

c. **I&A 3 Requirements.** In addition to I&A 2:

ISL 2007-01 #47 (8-607.c.). This paragraph requires “strong authentication” for privileged users that are either located or communicate outside the IS perimeter. In the context of the NISPOM, what constitutes “strong authentication?”

Answer: Strong authentication techniques provide countermeasures against common authentication attacks. This includes the use of cryptographic technologies (e.g., two factor tamper resistant hardware or software token authentication, digital signatures, etc.), one-time passwords, or biometric devices (retina, fingerprint, hand geometry, retina identification, etc.).

Consideration should be given to the use of a combination of technical (anomaly detection/prevention technologies, use of secure communication channels to mitigate eavesdropping, replay and session hijacking attacks) and non-technical measures (user education, enrollment procedures, authentication key management, etc.).

(1) Access to the IS by privileged users who either reside outside of the IS's perimeter or whose communications traverse data links that are outside the IS's perimeter shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks.)

d. **I&A 4 Requirements.** In those instances where the means of authentication is user-specified passwords, the ISSM may employ (with the approval of the CSA) automated tools to validate that the

passwords are sufficiently strong to resist cracking and other attacks intended to discover the user's password.

e. **I&A 5 Requirements.** In those instances where the users are remotely accessing the IS, the users shall employ a strong authentication mechanism.

8-608. Resource Control (ResrcCtrl). The system shall ensure that resources contain no residual data before being assigned, allocated, or reallocated.

8-609. Session Controls (SessCtrl). Session controls are requirements, over and above identification and authentication, for controlling the establishment of a user's session.

a. **SessCtrl 1 Requirements**

(1) User Notification. All users shall be notified prior to gaining access to a system that system usage is monitored, recorded, and subject to audit. The user shall also be advised that, by using the system, he/she has granted consent to such monitoring and recording. The user shall also be advised that unauthorized use is prohibited and subject to criminal and civil penalties. If the operating system permits, each initial screen (displayed before user logon) shall contain a warning text to the user and the user shall be required to take positive action to remove the notice from the screen (monitoring and recording, such as collection and analysis of audit trail information, shall be performed). The CSA will provide an approved banner. If it is not possible to provide an "initial screen" warning notice, other methods of notification shall be developed and approved by the CSA.

(2) Successive Logon Attempts. If the operating system provides the capability, successive logon attempts shall be controlled as follows:

(a) By denying access after multiple (maximum of five) consecutive unsuccessful attempts on the same user ID.

(b) By limiting the number of access attempts in a specified time period.

(c) By the use of a time delay control system.

(d) By other such methods, subject to approval by the CSA.

(3) System Entry. The system shall grant system entry only in accordance with the conditions associated with the authenticated user's profile. If no explicit entry conditions are defined, the default shall prohibit all remote activities, such as remote logons and anonymous file access.

b. **SessCtrl 2 Requirements.** In addition to SessCtrl 1:

(1). Multiple Logon Control. If the IS supports multiple logon sessions for each user ID or account, the IS shall provide a protected capability to control the number of logon sessions for each user ID, account, or specific port of entry. The IS default shall be a single logon session.

(2). User Inactivity. The IS shall detect an interval of user inactivity, such as no keyboard entries, and shall disable any future user activity until the user re-establishes the correct identity with a valid authenticator. The inactivity time period and restart requirements shall be documented in the SSP.

ISL 2007-01 #48 (8-609.b.(2)). What is the baseline time period of user inactivity and what procedures are required?

Answer: Users will be required to re-authenticate themselves (e.g., reenter password) after 15 minutes of user inactivity. If it is technically not feasible for the IS to implement this requirement, or the ISSM has implemented a time period longer than 15 minutes because of mission requirements, the GCA may accept this risk in a letter to the contractor. The ISSM will document this as a unique vulnerability in the applicable SSP as required by paragraph 8-610a(1)(c).

(3). Logon Notification. If the operating system provides the capability, the user shall be notified upon successful logon of: the date and time of the user's last logon; the location of the user (as can best be determined) at last logon; and the number of unsuccessful logon attempts using this user ID

since the last successful logon. This notice shall require positive action by the user to remove the notice from the screen.

8-610. Security Documentation (Doc). Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.

ISL 2007-01 #10 (8-202, 8-610). Is a Memorandum of Understanding (MOU) required when accredited mobile systems are relocated to government activities or test sites?

Answer: The contractor must have a signed letter from the GCA acknowledging acceptance of the relocation of the IS to the Government Activity prior to shipment. An MOU is not necessary unless the mobile system is connecting to an accredited government system.

a. Doc 1 Requirements

ISL 2007-01 #9 (8-201, 8-610.a.). These paragraphs requires the ISSM to certify that their IS have undergone a comprehensive evaluation of all technical and non-technical security features and safeguards. Is this all that is required for certification?

Answer: For the ISSM's certification, yes. However, to make such a certification, the ISSM must ensure that all other NISPOM required signatures identified in 8-610a as a Doc 1 requirement have been included. In addition, DSS can require an on-site validation of the ISSM's certification prior to the final accreditation of the system.

(1) SSP. The SSP shall contain the following:

(a) System Identification.

1. Security Personnel. The name, location, and phone number of the responsible system owner, CSA, ISSM, and ISSO.

2. Description. A brief narrative description of the system or network mission or purpose and architecture, including subnetworks, communications devices, and protocols.

(b) System Requirements Specification.

1. Sensitivity and Classification Levels. The sensitivity or classification levels, and categories of all information on the system and clearance, formal access approval and need-to-know of IS users.

2. Levels of Concern for Confidentiality, Integrity, and Availability. The confidentiality level of concern and protection level, the integrity level of concern, and the availability level of concern.

3. Protection Measures. Identify protection measures and how they are being met.

ISL 2009-01 #1 (8-101.a., 8-610.a.(1)(b)3). This Industrial Security Letter (ISL) pertains to the Defense Security Service (DSS) Office of Designated Approving Authority (ODAA) "Manual for the Certification and Accreditation of Classified Systems under the National Industrial Security Program Operating Manual (NISPOM)," hereafter referred to as the "Manual."

Use of the Manual will support contractor compliance with the NISPOM. The Manual sets forth guidance for contractors to use in developing their system security plans (SSPs) and continuous certification and accreditation requirements. The Manual implements and conforms to NISPOM requirements, and is based on other Federal standards* that apply to national security systems used by Government and contractors. Use of, and adherence to, the Manual will facilitate the DSS review of SSPs and IS certifications.

**These standards include: Department of Defense (DoD), National Security Agency (NSA), Defense Information System Agency (DISA), National Institute of Standards and Technology (NIST), and the Committee on National Security Systems (CNSS).*

The CNSS (see National Security Directive Number 42, and Executive Order (EO) 13231, October 16, 2001) is chaired by the Department of Defense and is charged with setting national policy, operational procedures and guidance for National Security Systems (NSS). The CNSS goal was a convergence of standards for the DoD, Intelligence, and civilian communities into one common, consistent process with one set of common standards for the federal security authorization process (i.e., certification and accreditation). Contractor IS used to process classified information are defined as national security systems (NSS) per the Federal Information Security Management Act (FISMA) of 2002 (44 U.S.C. §3541, et seq., which refers to the definition of NSS at 44 U.S.C. §3532(b)(2)).

By FISMA definition, NSS are those that are used or operated by an agency or by a contractor of an agency, or another organization on behalf of the agency, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon system, or are protected at all times by procedures established for information that have been specifically authorized under criteria established by an EO or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

The CNSS is also currently drafting the set of standards for NSS in draft CNSS Instruction 1253, "Security Control Catalog for National Security Systems". These CNSS security standards and guidelines are integrated into a risk management framework that promotes the concept of "near real-time risk management" based on continuous monitoring of information systems. As contractor IS used to process classified information are considered to be NSS, DSS anticipates that these CNSS standards will form the basis of any future revisions to NISPOM requirements pertaining to IS security.

4. Variances from Protection Measure Requirements. A description of any approved variances from protection measures. A copy of the approval documentation shall be attached to the SSP.

(c) System-Specific Risks and Vulnerabilities. A description of the risk assessment of any threats or vulnerabilities unique to the system. If there are no threats or vulnerabilities unique to the facility or system, a statement to that effect shall be entered. If any vulnerabilities are identified by the assessment of unique threats, the countermeasures implemented to mitigate the vulnerabilities shall be described.

ISL 2007-01 #21 (8-302.a., 8-305, 8-306.b., 8-309, 8-310.a. & b., 8-401, 8-610.a.(1)(c)). Can DSS provide additional guidance on the trusted download process and the requirement for output and media review?

Answer: Yes, Due to the diversity and uniqueness of the numerous vendor platforms and applications in use (e.g., word processing, database, electronic mail, and spreadsheets), a thorough review by the ISSM and DSS must be conducted before the trusted downloading procedures are used to create classified or unclassified electronic files and/or media.

All trusted downloading procedures must use new media. This mitigates the possibility of classified system contamination or corruption, as used media could contain and inadvertently introduce unauthorized software into the classified system.

The DSS Trusted Downloading Procedures can be found on the DSS web site (www.dss.mil) under the Industrial Security Program link. These procedures support many of the standard applications and can be used to examine information that is not in human readable form with the reasonable assurance that only the requested information was transferred.

If the ISSM is unable to implement the DSS procedures found on the DSS website, the System Security Plan (SSP) must (under the vulnerability reporting requirement of paragraph 8-610a(1)(c)) include a description of how and why the contractor has deviated from the standard, and a risk acceptance statement by the GCA.

Trusted Downloading Procedures do not need to be followed when classified information is transferred from an accredited PL 1 system storing the same level of classified information from multiple programs to media that will be handled and then remain at the same or higher level classified environment and controls (i.e., handling, marking, distribution/access controls, safeguarding, etc.). However, a review must be accomplished to ensure that only the designated files were transferred to the new media. This could include a review of hard copy output and/or a visual review of the electronic file.

(d) System Configuration. A brief description of the system architecture, including a block diagram of the components that show the interconnections between the components and any connections to other systems, and an information flow diagram.

(e) Connections to Separately Accredited Networks and Systems. If connections to other systems exist, a memorandum of understanding is necessary if the systems are approved by a person other than the CSA responsible for this system. A copy of any memoranda of understanding with other agencies shall be attached to the SSP.

(f) Security Support Structure. A brief description of the security support structure including all controlled interfaces, their interconnection criteria, and security requirements.

(2) Certification and Accreditation Documentation.

(a) Security Testing. Test plans, procedures, and test reports including risk assessment.

(b) Documentation. The test plan for ongoing testing and the frequency of such testing shall be documented in the SSP.

(c) Certification. A certification statement that the system complies with the requirements of the protection level and levels of concern for this system. The statement shall be signed by the ISSM.

(d) Accreditation. Documentation for accreditation includes the certification package. The CSA approves the package and provides accreditation documentation.

8-611. Separation of Function Requirements (Separation). At Protection Level 3 the functions of the ISSO and the system manager shall not be performed by the same person.

8-612. System Recovery (SR). System recovery addresses the functions that respond to failures in the SSS or interruptions in operation. Recovery actions ensure that the SSS is returned to a condition where all security-relevant functions are operational or system operation is suspended.

a. **SR 1 Requirements.** Procedures and IS features shall be implemented to ensure that IS recovery is done in a controlled manner. If any off-normal conditions arise during recovery, the IS shall be accessible only via terminals monitored by the ISSO or his/her designee, or via the IS console.

8-613. System Assurance (SysAssur). System assurance includes those components of a system (hardware, software, firmware, and communications) that are essential to maintaining the security policy(ies) of the system, (e.g. Security Support Structure).

a. **SysAssur 1 Requirements**

(1) Access to Protection Functions. Access to hardware/software/firmware that perform systems or security functions shall be limited to authorized personnel.

b. **SysAssur 2 Requirements.** In addition to SysAssur1:

(1) Protection Documentation. The protections and provisions of the SysAssur shall be documented.

(2) Periodic Validation of SysAssur. Features and procedures shall exist to periodically validate the correct operation of the hardware, firmware, and software elements of the SSS and shall be documented in the SSP.

c. **SysAssur 3 Requirements.** In addition to SysAssur2:

(1) SSS Isolation. The SSS shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modifying its code and data structures).

8-614. Security Testing (Test). Certification and ongoing security testing are the verification of correct operation of the protection measures in a system. The ISSM will perform and document the required tests.

ISL 2007-01 #7 (8-104.d., 8-614). Paragraph 8-104.d. requires that an IS certification test be developed and implemented. What is a certification test and when would it be required?

Answer: A certification test or process outlines the inspection and test procedures used to demonstrate compliance with the security requirements associated with the Protection Level (PL) assigned to the IS. The certification test is administered during the certification process and verifies correct operation of the protection measures in the IS. When the ISSM signs the Certification Test, he/she is affirming in writing that the system is currently installed and configured as described in the SSP. The DSS accreditation decision relies heavily on the accuracy of the ISSM's certification.

a. **Test 1 Requirements.** Assurance shall be provided to the CSA that the system operates in accordance with the approved SSP and that the security features, including access controls and configuration management, are implemented and operational.

ISL 2007-01 #49 (8-614.a.). What is the difference between Paragraph 8-614.a., which requires the ISSM provide "assurance" and paragraph 8- 614b where the ISSM is required to provide "written assurance"?

Answer: The assurance the ISSM provides under paragraph 8-614..a Test 1 is a statement in the SSP that the security features, including access controls and configuration management, are implemented and

operational. Under paragraph 8-614b Test 2 requirement, the ISSM provides written assurance to the CSA that the IS operates in accordance with the approved SSP and the individual verification that each of the requirements of Table 5 for technical security features and safeguards has been implemented and is operational to include access controls, configuration management and discretionary access controls.

b. **Test 2 Requirements.** In addition to Test1:

(1) Written assurance shall be provided to the CSA that the IS operates in accordance with the approved SSP, and that the security features, including access controls, configuration management and discretionary access controls, are implemented and operational.

c. **Test 3 Requirements.** In addition to Test2:

(1) Certification testing shall be conducted including verification that the features and assurances required for the Protection Level are functional.

(a) A test plan and procedures shall be developed and shall include:

1. A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and availability.

2. A detailed description of the assurances that have been implemented, and how this implementation will be verified.

3. An outline of the inspection and test procedures used to verify this compliance.

8-615. Disaster Recovery Planning. If disaster recovery planning is contractually mandated, the ISSM will develop a plan that identifies the facility's mission essential applications and information, procedures for the backup of all essential information and software on a regular basis, and testing procedures.

Section 7. Interconnected Systems

8-700. Interconnected Systems Management. The characteristics and capabilities of an IS implemented as networks require special security considerations. This section states additional requirements on a network or expands on the security requirements stated in Section 6 as they apply to a network.

ISL 2007-01 #50 (8-700). What are the overall PL2 network security requirements for interconnected Wide Area Networks (WAN) involving different classified programs, multiple contractor facilities, (i.e. individual nodes) under different need to know criteria?

Answer: Network security requirements for multiple nodes connected to a WAN are determined by the overall WAN DAA. The WAN DAA will determine the certification testing requirements for the WAN and individual nodes. The WAN DAA may determine that the combination of data and/or users on the interconnected network requires a higher PL than those of its nodes. Security requirements for these networks will address the following minimum requirements:

a) Each interconnected WAN node must be separately accredited and maintain its individual accreditation. All WAN nodes must be issued an Approval To Connect (ATC) by the WAN DAA before connecting to the WAN.

b) An approved overall Network Security Plan (NSP) and Network Protection Profile (NPP). The NSP and NPP are maintained and updated to reflect changes, topography, connections, new technologies and new Operating Systems as required.

c) When a connection to a government system is involved, the WAN DAA shall require the establishment of an MOU to document the need for the connection, connection requirements, all required approvals, and the certification and accreditation (C&A) roles and responsibilities of all WAN participants.

d) Each separately accredited system or network will maintain its own intra-system services and controls and protects its own resources.

e) Each participating system or network must have its own ISSO.

f) Utilization of a Controlled Interface (CI) to provide a protected conduit for the transfer of user data. The CI must be capable of adjudicating the different security policy implementations of the participating systems or unified networks, and must support the required protection requirements of the most restrictive attached WAN nodes.

ISL 2007-01 #51 (8-700, 8-701). Paragraphs 8-700 and 8-701 refer to the use of a Controlled Interface (CI) when connecting networks of the same or different classification levels. DoD uses the term “high assurance guard.” Are the terms “high assurance guard” (HAG) and “Controlled Interface” (CI) interchangeable?

Answer: No, there is some difference between these terms. The HAG is comprised of hardware and software that enforces the established security rules during transmission of message and directory traffic between enclaves of different classification levels. The CI is a mechanism that can actually adjudicate the different interconnected security policies (controls the flow of information in and out of the interconnected systems).

a. When connecting two or more networks, the CSA shall review the security attributes of each network (even if the networks are accredited at the same protection level) to determine whether the combination of data and/or the combination of users on the connected network requires a higher protection level.

b. A unified network is a connected collection of systems or networks that are accredited: (1) under a single SSP, (2) as a single entity, and (3) by a single CSA. Such a network can be as simple as a small stand-alone LAN operating at Protection Level 1, following a single security policy, accredited as a single entity, and administered by a single ISSO. Conversely, it can be as complex as a collection of hundreds of LANs separated over a wide area but still following a single security policy, accredited as a single entity by a single CSA. The perimeter of each network encompasses all its hardware, software, and

attached devices. Its boundary extends to all of its users.

c. An interconnected network is comprised of two or more separately accredited systems and/or networks. Each separately accredited system or network maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating system or network has its own ISSO. The interconnected network shall have a controlled interface capable of adjudicating the different security policy implementations of the participating systems or unified networks. An interconnected network also requires accreditation as a unit.

d. Systems that process information at differing classification levels or with differing compartmentation (i.e., at least two kinds of information that require different formal access approvals) can be interconnected if:

ISL 2007-01 #52 (8-700.d.). This paragraph states that interconnected systems (i.e., networks) can process information at different classification levels or different compartments. What are the required technical security features, safeguards and assurances?

Answer: The technical security features, safeguards and assurances for interconnected systems or networks require the use of a Controlled Interface (CI). The CI must have been evaluated and been found to meet the Evaluation Assurance Level 6 (EAL 6) level of trust under the National Information Assurance Partnership (NIAP) - NSA and National Institute of Standards and Technology (NIST) Common Criteria Evaluation and Validation Scheme (CCEVS).

The EAL 6 evaluations are a semiformal verification and testing of the IS eleven (11) standard categories of functional requirements and ten (10) categories of assurance requirements. The functional requirements include identification and authentication, protection of security functions, security management, privacy, user data protection (access control, information flow, etc.), communication protection (encryption, Public Key Information (PKI), non-repudiation, confidentiality, security audit, resource utilization, fault tolerance, etc.). The 10 assurance requirements

are a Protection Profile (PP) evaluation, Security Target (ST) evaluation, configuration management, development, test, delivery/operation, life cycle, guidance documents, vulnerability assessment, and maintenance of assurance requirements. EAL-6 corresponds roughly to the DoD (Trusted Computer System Evaluation Criteria (TCSEC) B3 level of trust functional and assurance requirements.

More information on the CCEVS can be found at URL: <http://www.niap-ccevs.org/cc-scheme/>.

ISL 2007-01 #53 (8-700.d.). Must the contractor use a Controlled Interface (CI) from the SECRET and Below Interoperability (SABI) Program when networks belonging only to contractors are interconnected at different classification levels or different compartments?

Answer: No. The contractor must use a CI meeting the DISA Global Information Assurance Program (GIAP) Cross Domain Solutions (CDS) Program requirements, which replaced the SABI connections process. For more information on DISA's CDS requirements, go to <http://iase.disa.mil/index2.html> or directly to CDS at: <http://iase.disa.mil/cds/index.html>

(1) They are interconnected through a Controlled Interface (as defined below) that provides the separation appropriate to the combination of the level(s) and compartment(s) being processed on both systems; or

(2) Both systems are operating at the same protection level (both systems must be accredited to protect the information being transferred); or

(3) Both systems are accredited to process the level(s) and compartment(s) of information that they will receive, and at least one system is accredited to provide appropriate separation for the information being transferred.

e. Any IS connected to another system that does not meet either d (2) or d (3) above shall utilize a Controlled Interface(s) (CI) that performs the following:

(1) A communication of lower classification level from within the system perimeter shall be reviewed for classification before being released.

(2) A classified communication from within the system perimeter shall have the body and attachments of the communication encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

(3) Communications from outside the system perimeter shall have an authorized user as the addressee (i.e., the CI shall notify the user of the communication and forward the communication only on request from the user). If classified information exists in the communication, it shall be encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

8-701. Controlled Interface Functions

ISL 2007-01 #51 (8-700, 8-701). Paragraphs 8-700 and 8-701 refer to the use of a Controlled Interface (CI) when connecting networks of the same or different classification levels. DoD uses the term “high assurance guard.” Are the terms “high assurance guard” (HAG) and “Controlled Interface” (CI) interchangeable?

Answer: No, there is some difference between these terms. The HAG is comprised of hardware and software that enforces the established security rules during transmission of message and directory traffic between enclaves of different classification levels. The CI is a mechanism that can actually adjudicate the different interconnected security policies (controls the flow of information in and out of the interconnected systems).

a. The functions of the CI include:

(1) Providing a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts.

(2) Providing a reliable exchange of security-related information.

(3) Filtering information in a data stream based on associated security labels for data content.

b. CIs have several characteristics including the following:

(1) There are no general users on the CI.

(2) There is no user code running on the CI.

(3) The CI provides a protected conduit for the transfer of user data.

(4) Communications from outside the perimeter of the system shall be reviewed for viruses and other malicious code.

8-702. Controlled Interface Requirements. The CI shall have the following properties:

a. Adjudicated Differences. The CI shall be implemented to monitor and enforce the protection requirements of the network and to adjudicate the differences in security policies.

b. Routing Decisions. The CI shall base its routing decisions on information that is supplied or alterable only by the SSS.

c. Restrictive Protection Requirements. The CI shall support the protection requirements of the most restrictive of the attached networks or IS.

d. User Code. The CI shall not run any user code.

e. Fail-secure. The CI shall be implemented so that all possible failures shall result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability.

f. Communication Limits. The CI shall ensure that communication policies and connections that are not explicitly permitted are prohibited.

g. In general, such systems have only privileged users; i.e., system administrators and maintainers. The CI may have a large number of clients (i.e., individuals who use the CI's functional capabilities in a severely constrained way). The CI application itself will have to provide the more stringent technical protections appropriate for the system's protection level. Multiple applications do not affect the overall protection provided by the CI if each application (and the resources associated with it) is protected from unauthorized access or circumvention from other applications or users.

8-703. Assurances for CIs. Each CI shall be tested and evaluated to ensure that the CI, as implemented, can provide the separation required for the system's protection level. Specifically, the platform on which the CI runs does not necessarily have to provide the needed separation alone.

CHAPTER 9 Special Requirements

Section 1. RD, FRD and Transclassified Foreign Nuclear Information (TFNI)

ISL 2006-01 #17 (Chapter 9 Section 1). This section was provided by DOE and applies to those contractors that are under DOE cognizance. It does not apply to contractors under DoD cognizance and should be considered as information only. Guidance on marking RD and FRD material must be included in the contract document. If adequate guidance has not been provided, the contractor should request assistance from the GCA.

9-100. General. This section was prepared by DOE according to reference (a) and is provided for information purposes only. It describes the requirements for classifying and safeguarding nuclear-related information that is designated RD or FRD or TFNI. Such information is classified under reference (c) as opposed to other Government information that is classified by E.O. (National Security Information (NSI)).

9-101. Authority and Responsibilities.

a. Reference (c) establishes policy for classifying and protecting RD, FRD, and TFNI information. Under section 141 of reference (c), DOE is responsible for controlling the dissemination and declassification of RD. Under section 142c and d of reference (c), DOE shares certain responsibilities regarding RD and FRD with the Department of Defense. Under section 142e of reference (c), DOE shares certain responsibilities regarding RD and TFNI with the DNI. Under section 143 of reference (c), the Secretary of Defense is responsible for establishing personnel and other security procedures and standards that are in reasonable conformity to the standards established by DOE. The procedures and standards established by the Secretary of Defense are detailed in other sections of the Manual and are applicable to contractors under the security cognizance of the Department of Defense.

b. Specific policies and procedures for classifying and declassifying RD and FRD are set forth in 10 Code of Federal Regulations (CFR) Part 1045, Subparts A, B, and C (reference (p)).

c. The Secretary of Energy and the Chairman of the NRC retain authority over access to information that is under their respective cognizance as directed by reference (c). The Secretary of DOE or the Chairman of the NRC may inspect and monitor contractor programs or facilities that involve access to such information or may enter into written agreement with the Department of Defense to inspect and monitor these programs or facilities.

9-102. Unauthorized Disclosures. Contractors shall report all unauthorized disclosures involving RD and FRD information to the CSA.

9-103. International Requirements. Reference (c) provides for a program of international cooperation to promote common defense and security and to make available to cooperating nations the benefits of peaceful applications of atomic energy as widely as expanding technology and considerations of the common defense and security will permit. Under section 123 of reference (c), information controlled by reference (c) may be shared with another nation only under the terms of an agreement for cooperation. The disclosure by a contractor of RD and FRD shall not be permitted until an agreement is signed by the United States and participating governments and disclosure guidance and security arrangements are established. RD and FRD shall not be transmitted to a foreign national or regional defense organization unless such action is approved and undertaken under an agreement for cooperation between the United States and the cooperating entity and supporting statutory determinations as prescribed in reference (c).

9-104. Personnel Security Clearances. Only DOE, NRC, Department of Defense, and NASA can grant access to RD and FRD. The minimum investigative requirements and standards for access to RD and FRD for contractors under the security cognizance of DOE are set forth below.

a. TOP SECRET RD – A favorable SSBI.

b. SECRET RD – A favorable SSBI.

c. CONFIDENTIAL RD – A favorable NACLC.

d. TOP SECRET FRD – A favorable SSBI.

e. SECRET FRD – A favorable NACLC.

f. CONFIDENTIAL FRD – A favorable NACLC.

9-105. Classification.

a. The Director, DOE, Office of Classification and Information Control, determines whether nuclear-related information is classified as RD under reference (p). DOE and the Department of Defense jointly determine what classified information is removed from the RD category to become FRD under section 14(a) of reference (p). These decisions are promulgated in classification guides issued under section 37(a) of reference (p).

b. Reference (p) describes the authorities and procedures for classifying RD and FRD information and documents. All contractors with access to RD and FRD shall designate specified employees as RD Classifiers. Only those contractor employees designated as RD classifiers may classify RD and FRD documents according to section 32(a)(2) of reference (p). Such employees must be trained on the procedures for classifying, declassifying, marking, and handling for RD and FRD information and documents according to section 35(a) of reference (p). RD classifiers shall use classification guides as the primary basis for classifying and declassifying documents containing RD and FRD information according to section 37(c) of reference (p). If such classification guidance is not available and the information in the document appears to meet the definition of RD, then the RD classifier shall, as an interim measure, mark the document as Confidential RD (or as Secret RD if the sensitivity of the information in the document so warrants) and promptly forward the document to the GCA. The GCA shall provide the contractor with the final determination based upon official published classification guidance. If the GCA cannot make such a determination, the GCA shall forward the document to DOE for a classification determination according to section 14(a) of reference (p).

c. Classifying information as RD and FRD is not limited to U.S. Government information. Contractors who develop an invention or discovery useful in the production or utilization of special nuclear material or nuclear energy shall file a fully descriptive report with DOE or the Commissioner of Patents as prescribed by Section 151c of reference (c). Documents thought to contain RD or FRD shall be marked temporarily as such. These documents shall be promptly referred to the GCA for a final determination based upon official published classification guidance. If the GCA cannot make such a determination, the GCA shall forward the document to DOE for a classification determination.

9-106. Declassification.

a. DOE determines whether RD and TFNI information may be declassified under section 14(b) of reference (p). DOE, jointly with the Department of Defense, determines whether FRD information may be declassified under section 14(d) of reference (p).

b. Documents marked as containing RD, FRD and TFNI information remain classified until a positive action by an authorized Government official is taken to declassify them; no date or event for automatic declassification ever applies to RD, FRD, and TFNI documents.

9-107. Challenges to RD/FRD Classification. Any contractor employee who believes that an RD, FRD, and TFNI document is classified improperly or unnecessarily may challenge that classification following the procedures established by the GCA.

9-108. Marking. Documents containing RD, FRD, and TFNI information shall be marked as indicated below:

a. Front of the Document. In addition to the overall classification level of the document at the top and bottom of the page, the following notices must appear on the front of the document, as appropriate:

If the document contains RD information:

RESTRICTED DATA

This document contains RESTRICTED DATA as defined in the Atomic Energy Act of 1954.

Unauthorized disclosure subject to
administrative and criminal sanctions.

If the document contains FRD information:

FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to
administrative and criminal sanctions. Handle as
Restricted Data in foreign dissemination.
Section 144b, AEA 1954.

A document containing RD or FRD information also
must be marked to identify: (1) the classification
guide or source document (by title and date) used to
classify the document and (2) the identity of the RD
classifier unless the classifier is the same as the
document originator or signer:

Derived from: (Classification guide or source
document – title and date)
RD Classifier: (Name and position or title)

b. Interior Page. Each RD or FRD document
must also be clearly marked at the top and bottom of
each interior page with the overall classification level
and category of the document or the classification
level and category of the page, whichever is
preferred. The abbreviations RD and FRD may be
used in conjunction with the classification level (e.g.,
SECRET RD or SECRET FRD).

c. Other Caveats. Any other caveats indicated
on the source document shall be carried forward.

d. TFNI. Documents containing TFNI must be
marked in accordance with reference (z) and ISOO
Notice 2011-02: Further Guidance and Clarification
on Commingling Atomic Energy Information and
Classification National Security Information
(reference (aa)).

9-109. Comingling. To the greatest degree possible,
do not comingle RD and FRD in the same document
with information classified pursuant to reference (b).
When mixing can't be avoided, the requirements of
references (b) and (z) must be met.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 2. DOD Critical Nuclear Weapon Design Information (CNWDI)

9-200. General. This section contains the special requirements for protection of CNWDI.

9-201. Background. CNWDI is a DoD category of TOP SECRET RD or SECRET RD that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test or replace. The sensitivity of DoD CNWDI is such that access shall be granted to the absolute minimum number of employees who require it for the accomplishment of assigned responsibilities on a classified contract. Because of the importance of such information, special requirements have been established for its control. DoD Instruction 5210.2 (reference (q)) establishes these controls in DoD.

9-202. Briefings. Prior to having access to DoD CNWDI, employees shall be briefed on its sensitivity by the FSO or his or her alternate. (The FSO will be initially briefed by a Government representative.) The briefing shall include the definition of DoD CNWDI, a reminder of the extreme sensitivity of the information, and an explanation of the individual's continuing responsibility for properly safeguarding DoD CNWDI, and for ensuring that dissemination is strictly limited to other personnel who have been authorized for access and have a need-to-know for the particular information. The briefing shall also be tailored to cover any special local requirements. Upon termination of access to DoD CNWDI, the employee shall be given an oral debriefing.

9-203. Markings. In addition to any other required markings, CNWDI material shall be clearly marked, "Critical Nuclear Weapon Design Information-DoD Instruction 5210.2 Applies." As a minimum, CNWDI documents shall show such markings on the cover or first page. Portions of documents that contain CNWDI shall be marked with an (N) or (CNWDI) following the classification of the portion; for example, TS(RD)(N) or TS(RD)(CNWDI).

9-204. Subcontractors. Contractors shall not disclose CNWDI to subcontractors without the prior written approval of the GCA. This approval may be included in a Contract Security Classification Specification, other contract-related document, or by separate correspondence.

9-205. Transmission Outside the Facility. Transmission outside the contractor's facility is authorized only to the GCA, or to a subcontractor as described in paragraph 9-204 above. Any other transmission must be approved by the GCA. Prior to transmission to another cleared facility, the contractor shall verify from the CSA that the facility has been authorized access to CNWDI. When CNWDI is transmitted to another facility, the inner wrapping shall be addressed to the personal attention of the FSO or his or her alternate, and in addition to any other prescribed markings, the inner wrapping shall be marked: "Critical Nuclear Weapon Design Information-DoD Instruction 5210.2 Applies." Similarly, transmissions addressed to the GCA or other U.S. Government agency shall bear on the inner wrapper the marking "Critical Nuclear Weapon Design Information-DoD Instruction 5210.2 Applies."

9-206. Records. Contractors shall annotate CNWDI access in the CSA-designated database for all employees who have been authorized access to CNWDI.

9-207. Weapon Data. That portion of RD or FRD that concerns the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of atomic weapons or atomic weapon components and nuclear explosive devices is called Weapon Data and it has special protection provisions. Weapon Data is divided into Sigma categories the protection of which is prescribed by DOE Order 452.8 (reference (r)). However, certain Weapon Data has been re-categorized as CNWDI and is protected as described in this section.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 3. Intelligence Information

ISL 2006-01 #18 (Chapter 9 Section 3). This section was provided by the Central Intelligence Agency (CIA) and should be considered as information only. Specific guidance on marking intelligence information must be included in the contract document. If adequate guidance has not been provided, the contractor should request assistance from the GCA.

9-300. Background. This section was prepared by CIA in accordance with reference (a) and is provided for information purposes only. It contains general information on safeguarding intelligence information. Intelligence information is under the jurisdiction and control of the DNI, who establishes security policy for the protection of intelligence information, sources, methods, and analytical processes.

9-301. Definitions. The following definitions pertain to intelligence information:

a. Counterintelligence (CI). Information collection, analysis and operations conducted to identify and neutralize espionage, other foreign intelligence or covert actions, the intelligence-related capabilities and activities of terrorists, and operations against U.S. personnel or political, economic and policy processes.

b. Classified Intelligence Information. Information identified as SCI included in SAPs for intelligence, and collateral classified intelligence information under the purview of the DNI.

c. Foreign Intelligence. Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence information except for information on international terrorist activities.

d. Intelligence Community (IC). Those U.S. Government organizations and activities identified as members of the IC in reference (e).

e. Senior Officials of the Intelligence Community (SOICs). SOICs are the heads of departments and agencies with organizations in the IC or the heads of IC organizations responsible for protecting classified intelligence information and

intelligence sources and methods from unauthorized disclosure consistent with DNI policy.

f. Senior Intelligence Officer (SIO). The SIO is the highest ranking military or civilian individual charges with direct foreign intelligence missions, functions, or responsibilities within an element of the IC.

g. SCI. SCI is classified intelligence information concerning or derived from sensitive sources, methods, or analytical processes, which is required to be handled exclusively within formal access control systems established by the DNI.

h. SCI Facility (SCIF). A SCIF is an area, room, group of rooms, or installation accredited by the proper authority to store, use, discuss and/or process SCI.

9-302. Key Concepts. This section provides general guidance on the intended purpose of several security tenets that form a critical baseline for the protection of intelligence information.

a. Apply Need-to-Know. Authorized holders (individuals or information systems) of classified intelligence information shall determine if prospective recipients (individuals or information systems) have the requisite clearances and accesses, and require knowledge of specific classified intelligence information in order to perform or assist in a lawful and authorized governmental function. To effectively implement this concept, IC departments, agencies, and bureaus must work cooperatively with customers to understand their requirements and ensure that they receive all applicable classified intelligence information while minimizing the risk of unauthorized disclosure. IC organizations shall provide intelligence at multiple security levels appropriate to the security authorizations of intended customers. Customers, in turn, shall be responsible for verifying need-to-know for this information for individuals of information systems within their organizations.

b. Protect SCI. In order to protect information regarding particularly fragile intelligence sources and methods, SCI has been established as the SAP for the

DNI. SCI must be protected in specific SCI control systems and shall be clearly defined and identified. The DNI has the sole authority to create or to discontinue SAPs, including SCI access control systems pertaining to intelligence sources and methods and classified intelligence activities (including special activities, but not including military operational, strategic, and tactical programs).

c. Educate the Work Force. SOICs shall establish formal security awareness training and education programs to ensure complete, common, and consistent understanding and application of security principles. Individuals shall be advised of their security responsibilities before receiving access to classified intelligence information and information systems. Annual refresher training is required to review security principles and responsibilities and to emphasize new security policies and practices developed from the preceding year.

d. Promote Security Reciprocity. To facilitate security reciprocity across the IC and industry, SOICs shall accept from other IC departments, agencies, and bureaus access eligibility determinations and accreditations of information systems and facilities except when an agency has documented information indicating that an employee, contractor, information system, or a facility does not meet DCID standards. Any exceptions to access eligibility determinations and accreditations of information systems and facilities must be noted in certifications to other agencies.

e. Promote Institutional Collaboration. Security elements of the IC shall work with intelligence production, counterintelligence, and law enforcement partners to identify and implement integrated responses to threats. Proactive collaboration among programs should synergize efforts to protect the U.S. population, national security assets, and classified intelligence information.

f. Manage Risk. IC departments, agencies and bureaus shall employ a risk management/risk analysis process to cost-effectively minimize the potential for loss of classified intelligence information or assets and the consequences should such loss occur. This methodology shall involve techniques to counter

threats, reduce vulnerabilities, and implement security countermeasures.

g. Minimize Insider Threat. All personnel who have access to classified intelligence information shall be thoroughly vetted, fully trained in their security responsibilities, appropriately supervised, and provided a secure work environment. CI and security management shall maintain aggressive programs to deter, detect, and support the apprehension and prosecution of those cleared personnel who endanger national security interests.

9-303 Control Markings Authorized for Intelligence Information

a. “DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR” (ORCON). Information bearing this marking may be disseminated within the headquarters and specified subordinate elements of the recipient organizations, including their contractors within government facilities. This information may also be incorporated in whole or in part into other briefings or products, provided the briefing or product is presented or distributed only to original recipients of the information and marked accordingly. Dissemination beyond headquarters and specified subordinate elements or to agencies other than the original recipients requires advanced permission from the originator.

b. “FOR OFFICIAL USE ONLY” (FOUO). Intelligence information used to control dissemination of UNCLASSIFIED official government information until approved for public release by the originator. May be used only with UNCLASSIFIED on page markings.

c. “CAUTION-PROPRIETARY INFORMATION INVOLVED” (PROPIN). Marking used to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value. This information may not be disseminated outside the Federal Government in any form without the express permission of the originator of the proprietary information. Dissemination to contractors is precluded irrespective of their status to, or within, the

U.S. Government without the authorization of the originator of the information.

d. “NOT RELEASABLE TO FOREIGN NATIONALS” (NOFORN). NOFORN is classified information that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator. It cannot be used with REL TO [country codes] or EYES ONLY on page markings. When a document contains both NOFORN and REL TO (see below) or NOFORN and EYES ONLY portions, NOFORN takes precedence for the markings at the top and bottom of the page.

e. “AUTHORIZED FOR RELEASE TO (REL TO) (name of country (ies)/international organization)”. This marking is used to identify Intelligence Information that an originator has predetermined to be releasable or has released, through established foreign disclosure procedures and channels, to the foreign/international organization indicated.

9-304. Limitation on Dissemination of Classified Intelligence Information. A contractor is not authorized to further disclose or release classified intelligence information (including release to a subcontractor) without prior written authorization of the releasing agency.

9-305. Safeguarding Classified Intelligence Information. All classified intelligence information in the contractor’s possession shall be safeguarded and controlled according to the provisions of this manual for classified information of the same classification level, with any additional requirements and instructions received from the GCA, and with any specific restrictive markings or limitations that appear on the documents themselves.

9-306. Inquiries. All inquiries concerning source, acquisition, use, control, or restrictions pertaining to classified intelligence information shall be directed to the providing agency.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 4. Communications Security (COMSEC)

9-400. General. This section was prepared by NSA. The procedures in this section pertaining to COMSEC information shall apply to contractors when the contractor requires the use of COMSEC systems in the performance of a contract; the contractor is required to install, maintain, or operate COMSEC equipment for the U.S. Government; or the contractor is required to accomplish research, development, or production of COMSEC systems, COMSEC equipment, or related COMSEC material.

9-401. Instructions. Specific requirements for the management and safeguarding of COMSEC material in industry are established in the COMSEC material control and operating procedures provided to the custodian of each industrial COMSEC account by the agency Central Office of Record (COR) responsible for establishing the account. Such procedures that are above the baseline requirements detailed in the other sections of this manual shall be contractually mandated.

9-402. Clearance and Access Requirements

a. Before a COMSEC account can be established and a contractor may receive or possess COMSEC material accountable to a COR, individuals occupying the positions of FSO, COMSEC custodian, and alternate COMSEC custodian must have a final PCL appropriate for the material to be held in the account. COMSEC custodians and alternate COMSEC custodians having access to TOP SECRET keying material marked as containing CRYPTOGRAPHIC (CRYPTO) information must have a final security clearance based upon an SSBI current within five years. This requirement does not apply to contractors using only data transfer devices and seed key.

b. Before disclosure of COMSEC information to a contractor, GCAs must first verify with the CSA that appropriate COMSEC procedures are in place at the contractor facility. If procedures are not in place, the GCA shall provide a written request and justification to the CSA to establish COMSEC procedures and a COMSEC account, if appropriate, at the facility and to conduct the initial COMSEC briefings for the FSO and custodians.

c. Access to COMSEC information by a contractor requires a final FCL and a government-issued final PCL at the appropriate level; however, an Interim TOP SECRET FCL or PCL is valid for access to COMSEC at the SECRET and CONFIDENTIAL levels.

d. If a COMSEC account will be required, the Contract Security Classification Specification shall contain a statement regarding the establishment of a COMSEC account as appropriate.

9-403. Establishing a COMSEC Account

a. When COMSEC material which is accountable to a COR is to be provided, acquired or produced under a contract, the contracting officer shall inform the contractor that a COMSEC account must be established. The contractor shall forward the names of U.S. citizen employees who will serve as the COMSEC Custodian and Alternate COMSEC Custodian to the CSA. The CSA shall forward the names of the FSO, COMSEC Custodian, and Alternate Custodian to the appropriate COR, with a copy to the GCA, indicating that the persons have been cleared and COMSEC has been briefed.

b. The COR will then establish the COMSEC account and notify the CSA that the account has been established.

c. An individual may be appointed as the COMSEC custodian for more than one account only when approved by each COR concerned.

9-404. COMSEC Briefing and Debriefing Requirements

a. All contractor employees who require access to classified COMSEC information in the performance of their duties shall be briefed before access is granted. Depending on the nature of COMSEC access required, either a COMSEC briefing or a Cryptographic Access Briefing will be given. The FSO, the COMSEC Custodian, and the Alternate Custodian shall be briefed by a government representative or their designee. Other contractor employees shall be briefed by the FSO, the COMSEC Custodian, the Alternate Custodian, or other

individual designated by the FSO. The purpose of the briefing is to ensure that the contractor understands:

(1) The unique nature of COMSEC information and its unusual sensitivity,

(2) The special security requirements for the handling and protection of COMSEC information, and

(3) The penalties prescribed in Title 18, U.S.C., §§ 793, 794, and 798 (reference (s)) for willful disclosure of COMSEC information.

b. COMSEC debriefings are not required.

c. The contractor shall maintain a record of all COMSEC briefings.

9-405. CRYPTO Access Briefing and Debriefing Requirements

a. U.S. classified CRYPTO information is defined as:

(1) TOP SECRET and SECRET, CRYPTO, key and authenticators that are designated CRYPTO, and

(2) CRYPTO media that embody, describe, or implement classified CRYPTO logic; this includes full maintenance manuals, CRYPTO descriptions, drawings of a CRYPTO logic, specifications describing a CRYPTO logic, CRYPTO computer software, or any other media which may be specifically identified.

b. U.S. classified CRYPTO information does not include seed key and CCI.

c. A contractor's employee may be granted access to U.S. classified CRYPTO information only if the employee:

(1) Is a U.S. citizen;

(2) Has a final government-issued security clearance appropriate to the classification of the U.S. CRYPTO information to be accessed;

(3) Has a valid need-to-know to perform duties for, or on behalf of, the U.S. Government;

(4) Receives a security briefing appropriate to the U.S. classified CRYPTO information to be accessed;

(5) Acknowledges the granting of access by executing Section I of Secretary of Defense Form (SD) 572, Cryptographic Access Certification and Termination; and

(6) Where so directed by a U.S. Government Department or Agency head, acknowledges the possibility of being subject to a non-lifestyle, CI-scope polygraph examination that shall be administered in accordance with department or agency directives and applicable law.

d. An employee granted access to CRYPTO information shall be debriefed and execute Section II of the SD 572 not later than 90 days from the date access is no longer required.

e. The contractor shall maintain the SD 572 for a minimum of three years following the debriefing.

f. CRYPTO access briefings fully meet the requirements of paragraph 9-407 of this manual for COMSEC briefings.

9-406. Destruction and Disposition of COMSEC Material. The COR shall provide directions to the contractor when accountable COMSEC material is to be destroyed. These directions may be provided in superseding editions of publications or by specific instructions.

9-407. Subcontracting COMSEC Work. Subcontracts requiring the disclosure of classified COMSEC information shall be awarded only upon the written approval of the GCA.

9-408. Unsolicited Proposals. Any unsolicited proposal for a COMSEC system, equipment, development, or study that may be submitted by a contractor to a government agency shall be forwarded to the Deputy Director, Information Systems Security, NSA, Fort George G. Meade, MD 20755-6000, for review and appropriate follow-up action.

CHAPTER 10

International Security Requirements

Section 1. General and Background Information

10-100. General. This Chapter provides policy and procedures governing the control of classified information in international programs.

10-101. Applicable Federal Laws. The transfer of articles and services and related technical data to a foreign person, within or outside the U.S., or the movement of such material or information to any destination outside the legal jurisdiction of the U.S. constitutes an export. Depending on the nature of the articles or data, most exports are governed by the Arms Export Control Act (AECA) (reference (t)), the Export Administration Act (EAA) (reference (u)), and reference (c).

10-102. Bilateral Security Agreements. Bilateral security agreements are negotiated with various foreign governments. Confidentiality requested by some foreign governments prevents a listing of the countries that have executed these agreements.

ISL 2006-02 #21 (10-102). (ISL96L-1 #1). The NISPOM refers to a variety of security agreements negotiated between various governments. How do the terms of these agreements apply to contractors?

General Security of Military Information Agreements (GSOMIA) are negotiated by the United States with a foreign government and obligate each government to provide substantially the same degree of protection to each other's classified information. On occasion, annexes to the GSOMIA, called Industrial Security Agreements, are negotiated with the foreign government for handling classified information entrusted to industry. Program agreements (e.g., co-production) either reference the GSOMIA and Industrial Security Agreement or include security language that is substantially the same as that in those agreements. Further requirements are contained in NATO security regulations. The requirements in

Chapter 10 also are drawn from the security agreements and NATO regulations. Therefore, Chapter 10 obligates contractors to comply with the security requirements of the agreement, albeit indirectly.

a. The General Security Agreement, negotiated through diplomatic channels, requires that each government provide to the classified information provided by the other substantially the same degree of protection as the releasing government. The Agreement contains provisions concerning limits on the use of each government's information, including restrictions on third party transfers and proprietary rights. It does not commit governments to share classified information, nor does it constitute authority to release classified material to that government. It satisfies, in part, the eligibility requirements of reference (t) concerning the agreement of the recipient foreign government to protect U.S. classified defense articles and technical data. (The General Security Agreement also is known as a General Security of Information Agreement and General Security of Military Information Agreement. The title and scope are different, depending on the year the particular agreement was signed.)

b. Industrial security agreements have been negotiated with certain foreign governments that identify the procedures to be used when foreign government information is provided to industry. The Office of the Under Secretary of Defense (Policy) negotiates Industrial Security Agreements as an Annex to the General Security Agreement and the Director, DSS, has been delegated authority to implement the provisions of the Industrial Security Agreements. The Director of Security, NRC, negotiates and implements these agreements for the NRC.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 2. Disclosure of U.S. Information to Foreign Interests

10-200. Authorization for Disclosure. Disclosure guidance will be provided by the GCA. Disclosure authorization may be in the form of an export license, a technical assistance agreement, a manufacturing license agreement, a letter of authorization from the U.S. Government licensing authority, or an exemption to the export authorization requirements. Disclosure guidance provided for a previous contract or program shall not be used unless the contractor is so instructed in writing by the GCA or the licensing authority. Classified information normally will be authorized for disclosure and export as listed below:

a. Government-to-Government International Agreements. Classified information shall not be disclosed until agreements are signed by the participating governments and disclosure guidance and security arrangements are established. The export of technical data pursuant to such agreements may be exempt from licensing requirements of the International Traffic in Arms Regulation (ITAR) (reference (v)).

b. Symposia, Seminars, Exhibitions, and Conferences. Appropriately cleared foreign nationals may participate in classified gatherings if authorized by the Head of the U.S. Government Agency that authorizes the conduct of the conference.

c. Foreign Visits. Disclosure of classified information shall be limited to that specific information authorized in connection with an approved visit request or export authorization.

d. Temporary Exports. Classified articles (including articles that require the use of classified information for operation) exported for demonstration purposes shall remain under U.S. control. The request for export authorization shall include a description of the arrangements that have been made in-country for U.S. control of the demonstrations and secure storage under U.S. Government control.

10-201. Direct Commercial Arrangements. The disclosure of classified information may be authorized pursuant to a direct commercial sale only if the proposed disclosure supports a U.S. or foreign government procurement requirement, a government

contract, or an international agreement. A direct commercial arrangement includes sales, loans, leases, or grants of classified items, including sales under a government agency sales financing program. If a proposed disclosure is in support of a foreign government requirement, the contractor should consult with U.S. in-country officials (normally the U.S. Security Assistance/Armaments Cooperation Office or Commercial Counselor). An export authorization is required before a contractor makes a proposal to a foreign interest that involves the eventual disclosure of U.S. classified information. The contractor should obtain the concurrence of the GCA before submitting an export authorization request.

10-202. Contract Security Provisions.

a. When a U.S. contractor is authorized to award a subcontract or enter into a Manufacturing License Agreement, Technical Assistance Agreement, or other direct commercial arrangement with a foreign contractor that will involve classified information, security provisions will be incorporated in the subcontract document or agreement and security classification guidance via a Contract Security Classification Specification will be provided. A copy of the signed contract with the provisions and the classification guidance shall be provided to the CSA. If the export authorization specifies that additional security arrangements are necessary for performance on the contract, contractor developed arrangements shall be incorporated in appropriate provisions in the contract or in a separate security document.

b. The contractor shall prepare and maintain a written record that identifies the originator or source of classified information that will be used in providing defense articles or services to foreign customers. The contractor shall maintain this listing with the contractor's record copy of the pertinent export authorization.

c. Security provisions, substantially as shown below, shall be included in all contracts and subcontracts involving classified information that are awarded to foreign contractors.

(1) All classified information and material furnished or generated under this contract shall be protected as follows:

(a) The recipient will not release the information or material to a third-country government, person, or firm without the prior approval of the releasing government.

(b) The recipient will afford the information and material a degree of protection equivalent to that afforded it by the releasing government; and

(c) The recipient will not use the information and material for other than the purpose for which it was furnished without the prior written consent of the releasing government.

(2) Classified information and material furnished or generated under this contract shall be transferred through government channels or other channels specified in writing by the Governments of the United States and (insert applicable country) and only to persons who have an appropriate security clearance and an official need for access to the information in order to perform on the contract.

(3) Classified information and material furnished under this contract will be remarked by the recipient with its government's equivalent security classification markings.

(4) Classified information and material generated under this contract must be assigned a security classification as specified by the contract security classification specifications provided with this contract.

(5) All cases in which it is known or there is reason to believe that classified information or material furnished or generated under this contract has been lost or disclosed to unauthorized persons shall be reported promptly and fully by the contractor to its government's security authorities.

(6) Classified information and material furnished or generated pursuant to this contract shall not be further provided to another potential contractor or subcontractor unless:

(a) A potential contractor or subcontractor which is located in the United States or (insert applicable country) has been approved for access to classified information and material by U.S. or (insert applicable country) security authorities; or,

(b) If located in a third country, prior written consent is obtained from the United States Government.

(7) Upon completion of the contract, all classified material furnished or generated pursuant to the contract will be returned to the U.S. contractor or be destroyed.

(8) The recipient contractor shall insert terms that substantially conform to the language of these provisions, including this one, in all subcontracts under this contract that involve access to classified information furnished or generated under this contract.

Section 3. Foreign Government Information (FGI)

10-300. General. The contractor shall notify the CSA when awarded contracts by a foreign interest that will involve access to classified information. The CSA shall administer oversight and ensure implementation of the security requirements of the contract on behalf of the foreign government, including the establishment of channels for the transfer of classified material.

10-301. Contract Security Requirements. The foreign entity that awards a classified contract is responsible for providing appropriate security classification guidance and any security requirements clauses. The failure of a foreign entity to provide classification guidance shall be reported to the CSA.

10-302. Marking Foreign Government Classified Material.

a. Foreign government classified information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the government entity that furnished the information. The equivalent U.S. classification and the country of origin shall be marked on the front and back in English.

10-303. Foreign Government RESTRICTED Information and "In Confidence" Information.

ISL 2006-01 #19 (10-303). Protection and marking requirements for foreign government RESTRICTED and "In Confidence" information are to be incorporated into the contract by the foreign government. If such guidance has not been provided the contractor should contact DSS for assistance.

The requirement to protect foreign government RESTRICTED as U.S. CONFIDENTIAL must be specifically required by the foreign government and so indicated in the contract. If the contract does not include this protection requirement, the RESTRICTED and "In Confidence" information does not need to be protected as classified. However, the information shall not be disclosed to anyone except personnel who require access in connection with the contract.

a. Some foreign governments have a fourth level of classification that does not correspond to an equivalent U.S. classification that is identified as RESTRICTED Information. In many cases, bilateral security agreements require RESTRICTED information to be protected as U.S. CONFIDENTIAL information.

b. Some foreign governments may have a category of unclassified information that is protected by law. This latter category is normally provided to other governments on the condition that the information is treated "In Confidence." The foreign government or international organization must state that the information is provided in confidence and that it must be protected from release. A provision of Title 10 of the U.S. Code (reference (w)) protects information provided "In Confidence" by foreign governments or international organizations to the Department of Defense which is not classified but meets special requirements stated in section 130c reference (w). This provision also applies to RESTRICTED information which is not required by a bilateral agreement to be protected as classified information. The contractor shall not disclose information protected by this statutory provision to anyone except personnel who require access to the information in connection with the contract.

c. It is the responsibility of the foreign entity that awards the contract to incorporate requirements for the protection and marking of RESTRICTED or "In Confidence" information in the contract. The contractor shall advise the CSA if requirements were not provided by the foreign entity.

10-304. Marking U.S. Documents Containing FGI

a. U.S. documents containing foreign government information shall be marked on the front, "THIS DOCUMENT CONTAINS (indicate country of origin) INFORMATION." In addition, the portions shall be marked to identify both the country and classification level, e.g., (UK-C); (GE-C). The "Derived From" line shall identify U.S. as well as foreign classification sources.

b. If the identity of the foreign government must be concealed, the front of the document shall be

marked "THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION;" paragraphs shall be marked FGI, together with the classification level, e.g., (FGI-C); and the "Derived From" line shall indicate FGI in addition to any U.S. source. The identity of the foreign government shall be maintained with the record copy of the document.

c. A U.S. document, marked as described herein, shall not be downgraded below the highest level of foreign government information contained in the document or be declassified without the written approval of the foreign government that originated the information. Recommendations concerning downgrading or declassification shall be submitted to the GCA or foreign government contracting authority, as applicable.

10-305. Marking Documents Prepared For Foreign Governments. Documents prepared for foreign governments that contain U.S. and foreign government information shall be marked as prescribed by the foreign government. In addition, they shall be marked on the front, "THIS DOCUMENT CONTAINS UNITED STATES CLASSIFIED INFORMATION." Portions shall be marked to identify the U.S. classified information.

10-306. Storage and Control. Foreign government material shall be stored and access shall be controlled generally in the same manner as U.S. classified material of an equivalent classification. Foreign government material shall be stored in a manner that will avoid commingling with other material which may be accomplished by establishing separate files in a storage container.

ISL 2006-02 #23 (10-306). Q&A re Storage of Foreign Government Information on an Information System (revised from ISL 05L-1). NISPOM paragraph 10-306 requires that foreign government information be controlled generally in the same manner as U.S. classified material of an equivalent classification, and stored to avoid commingling with other material. This storage requirement is normally accomplished by establishing separate files in a storage container.

This requirement also applies to foreign government information stored on an information system. The preferable method for accomplishing this is to use

periods processing with separate drives. Other options include: separating the foreign government information into different directories or folders on the system and protecting the foreign government information storage locations; or use of mandatory access controls (MAC) to label the data and control its location on the system;

However, there are instances where the contract actually requires foreign government and other classified information to be commingled in an information system; for example, in connection with a joint international program. If commingling is required, files must be marked to allow identification of foreign government information.

10-307. Disclosure and Use Limitations. Foreign government information is provided by the foreign government to the United States. It shall not be disclosed to nationals of a third country, or to any other third party, or be used for other than the purpose for which it was provided without the prior written consent of the originating foreign government. Requests for other uses or further disclosure shall be submitted to the GCA for U.S. contracts, and through the CSA for direct commercial contracts. Approval of the request by the foreign government does not eliminate the requirement for the contractor to obtain an export authorization.

ISL 2006-02 #22 (10-307, 10-509 and Appendix C). Definitions of "Foreign National" and "U.S. Person, (ISL96L-1 #3). The NISPOM definition of a "U.S. person" is different from the definition found in the State Department's International Traffic in Arms Regulation (ITAR). Only a U.S. citizen is eligible for a personnel security clearance. Therefore, the NISPOM definition of U.S. person is an individual who is a U.S. citizen. The ITAR uses a broader definition of U.S. person based on a person's right to be hired if he or she is qualified for a job (employment). Such employment does not establish the eligibility basis for a security clearance.

Procedures must be in place to ensure that non-U.S. citizens do not have access to U.S. classified and foreign government information. If the procedures to preclude such access are not deemed adequate by the IS Rep, a detailed Technology Control Plan will be required that includes special briefings, non-

disclosure statements and more stringent access control measures.

10-308. Transfer. Foreign government information shall be transferred within the U.S. and its territories using the same channels as specified by this manual for U.S. classified information of an equivalent classification, except that non-cleared express overnight carriers shall not be used.

10-309. Reproduction. The reproduction of foreign government TOP SECRET information requires the written approval of the originating government.

10-310. Disposition. Foreign government information shall be destroyed on completion of the contract unless the contract specifically authorizes retention or return of the information to the GCA or foreign government that provided the information. TOP SECRET destruction must be witnessed and a destruction certificate executed and retained for 2 years.

10-311. Reporting of Improper Receipt of Foreign Government Material. The contractor shall report

to the CSA the receipt of classified material from foreign interests that is not received through government channels.

10-312. Subcontracting

a. A U.S. contractor may award a subcontract that involves access to FGI to another U.S. contractor, except as described in subparagraph b, on verifying with the CSA that the prospective subcontractor has the appropriate FCL and storage capability. The contractor awarding a subcontract shall provide appropriate security classification guidance and incorporate the pertinent security provisions in the subcontract.

b. Subcontracts involving FGI shall not be awarded to a contractor in a third country or to a U.S. company with a limited FCL based on third-country ownership, control, or influence without the express written consent of the originating foreign government. The CSA will coordinate with the appropriate foreign government authorities.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 4. International Transfers

10-400. General. This section contains the procedures for international transfers of classified material. The requirements in this section do not apply to the transmission of classified material to U.S. Government activities outside the United States.

10-401. International Transfers of Classified Material.

ISL 2006-01 #20 (10-401). The requirement for the U.S. Designated Government Representative (DGR) to be a U.S. Government employee has been eliminated. This change permits DSS to authorize the contractor's FSO, empowered official (as defined by the International Traffic in Arms Regulations (ITAR)), or other knowledgeable individual to act as the DGR for international transfers of classified material.

a. All international transfers of classified material shall take place through channels approved by both governments. Control of classified material must be maintained until the material is officially transferred to the intended recipient government through its designated government representative (DGR).

b. To ensure government control, written transmission instructions shall be prepared for all international transfers of classified material. Preparation of the instructions shall be the responsibility of the contractor for direct commercial arrangements, and the GCA for government arrangements.

c. The CSA shall be contacted at the earliest possible stage in deliberations that will lead to the international transfer of classified material. The CSA shall advise the contractor on the transfer arrangements, identify the recipient government's DGR, appoint a U.S. DGR, and ensure that the transportation plan prepared by the contractor or foreign government is adequate.

d. Requests for export authorizations that will involve the transfer of classified material shall be accompanied by a Department of State Form DSP-83, Non-Transfer and Use Certificate. The form shall be signed by an official of the responsible foreign

government who has the authority to certify that the transfer is for government purposes and that the classified material will be protected in compliance with a government-approved security agreement.

10-402. Transfers of Freight

ISL 2006-01 #15 (5-412 and 10-402). Escorts and Transfers of Freight. The requirement for escorts for classified shipments applies only when an escort is determined to be necessary to ensure the protection of classified information during transport.

NISPOM paragraph 10-402 discusses transportation plans and the conditions under which international carriers (e.g., commercial airlines) may be used to transport classified material internationally. The requirement for an escort is a matter to be determined by the U.S. approving authority for the transportation plan in consultation with the foreign government counterpart. Therefore, depending on specific circumstances and the judgment of the U.S. and foreign government approvers of the transportation plan, cleared escorts may or may not be required for international transfers.

a. Transportation Plan (TP). A requirement to prepare a TP shall be included in each arrangement that involves the international transfer of classified material as freight. The TP shall describe arrangements for the secure shipment of the material from the point of origin to the ultimate destination. The U.S. and recipient government DGRs shall be identified in the TP as well as any requirement for an escort. The TP shall provide for security arrangements in the event the transfer cannot be made promptly. When there are to be repetitive shipments, a Notice of Classified Consignment will be used.

b. Government Agency Arrangements. Classified material to be furnished to a foreign government under such transactions normally will be shipped via government agency-arranged transportation and be transferred to the foreign government's DGR within the recipient government's territory. The government agency that executes the arrangement is responsible, in coordination with the recipient foreign government, for preparing a TP.

When the point of origin is a U.S. contractor facility, the GCA shall provide the contractor a copy of the TP and the applicable Letter of Offer and Acceptance (LOA). If a freight forwarder is to be used in processing the shipment, the freight forwarder shall be provided a copy of the TP by the GCA.

c. Commercial Arrangements. The contractor shall prepare a TP in coordination with the receiving government. This requirement applies whether the material is to be moved by land, sea, or air, and applies to U.S. and foreign classified contracts. After the CSA approves the TP, it shall be forwarded to the recipient foreign government security authorities for final coordination and approval.

d. International Carriers. The international transfer of classified material shall be made using only ships, aircraft, or other carriers that:

- (1) Are owned or chartered by the U.S. Government or under U.S. registry,
- (2) Are owned or chartered by or under the registry of the recipient government, or
- (3) Are carriers other than those described that are expressly authorized to perform this function in writing by the Designated Security Authority of the GCA and the security authorities of the foreign government involved. This authority shall not be delegated and this exception may be authorized only when a carrier described in (1) or (2) above is not available and/or an urgent operational requirement dictates use of the exception.

10-403. Return of Material for Repair, Modification, or Maintenance. A foreign government or contractor may return classified material to a U.S. contractor for repair, modification, or maintenance. The approved methods of return shall be specified in either the GCA sales arrangement, the security requirements section of a direct commercial sales arrangement, or, in the case of material transferred as freight, in the original TP. The contractor, on receipt of notification that classified material is to be received, shall notify the applicable CSA.

10-404. Use of Freight Forwarders.

a. A commercial freight forwarder may be used to arrange for the international transfer of classified material as freight. The freight forwarder must be under contract to a government agency, U.S. contractor, or the recipient foreign government. The contract shall describe the specific functions to be performed by the freight forwarder. The responsibility for security and control of the classified material that is processed by freight forwarders remains with the U.S. Government until the freight is transferred to a DGR of the recipient government.

b. Only freight forwarders that have a valid FCL and storage capability at the appropriate level are eligible to take custody or possession of classified material for delivery as freight to foreign recipients. Freight forwarders that only process unclassified paperwork and make arrangements for the delivery of classified material to foreign recipients do not require an FCL.

10-405. Handcarrying Classified Material. To meet contractual requirements, the CSA may authorize contractor employees to handcarry classified material outside the United States. SECRET is the highest level of classified material to be carried and it shall be of such size and weight that the courier can retain it in his or her possession at all times. The CSA shall ensure that the contractor has made necessary arrangements with U.S. airport security and customs officials and that security authorities of the receiving government approve the plan. If the transfer is under a contract or a bilateral or multinational government program, the request shall be approved in writing by the GCA. The CSA shall be notified by the contractor of a requirement under this section at least 5 work days in advance of the transfer. In addition:

- a. The courier shall be a full-time, appropriately cleared employee of the dispatching contractor.
- b. The courier shall be provided with a Courier Certificate that shall be consecutively numbered and be valid for one journey only. The journey may include more than one stop if approved by the CSA and secure Government storage has been arranged at each stop. The Courier Certificate shall be returned

to the dispatching security officer immediately on completion of the journey.

c. Before commencement of each journey, the courier shall read and initial the Notes to the Courier attached to the Courier Certificate and sign the Courier Declaration. The Declaration shall be maintained by the FSO until completion of the next security inspection by the CSA.

d. The material shall be inventoried, and shall be wrapped and sealed in the presence of the U.S. DGR. The address of the receiving security office and the return address of the dispatching company security office shall be shown on the inner envelope or wrapping. The address of the receiving government's DGR shall be shown on the outer envelope or wrapping along with the return address of the dispatching office.

e. The dispatching company security office shall prepare three copies of a receipt based on the inventory and list the classified material involved. One copy of the receipt shall be retained by the dispatching company security office. The other two copies shall be packed with the classified material. The security office shall obtain a receipt for the sealed package from the courier.

f. The dispatching company security office shall provide the receiving security office with 24 work hours advance notification of the anticipated date and time of the courier's arrival and the identity of the courier. The receiving security office shall notify the dispatching company security office if the courier does not arrive within 8 hours of the expected time of arrival. The dispatching security office shall notify its DGR of any delay, unless officially notified otherwise of a change in the courier's itinerary.

g. The receiving DGR shall verify the contents of the consignment and shall sign the receipts enclosed in the consignment. One copy shall be returned to the courier. On return, the courier shall provide the executed receipt to the dispatching security office.

h. Throughout the journey, the consignment shall remain under the direct personal control of the courier. It shall not be left unattended at any time during the journey, in the transport being used, in hotel rooms, in cloakrooms, or other such location,

and it may not be deposited in hotel safes, luggage lockers, or in luggage offices. In addition, envelopes and packages containing the classified material shall not be opened en route, unless required by customs or other government officials.

i. When inspection by government officials is unavoidable, the courier shall request that the officials provide written verification that they have opened the package. The courier shall notify the FSO as soon as possible. The FSO shall notify the U.S. DGR. If the inspecting officials are not of the same country as the dispatching security office, the designated security authority in the country whose officials inspected the consignment shall be notified by the CSA. Under no circumstances shall the classified consignment be handed over to customs or other officials for their custody.

j. When carrying classified material, the courier shall not travel by surface routes through third countries, except as authorized by the CSA. The courier shall travel only on carriers described in 10-402d, and travel direct routes between the U.S. and the destination.

10-406. Classified Material Receipts. There shall be a continuous chain of receipts to record international transfers of all classified material from the contractor through the U.S. DGR and the recipient DGR to the ultimate foreign recipient. The contractor shall retain an active suspense record until return of applicable receipts for the material. A copy of the external receipt that records the passing of custody of the package containing the classified material shall be retained by the contractor and each intermediate consignee in a suspense file until the receipt that is enclosed in the package is signed and returned. Follow-up action shall be initiated through the CSA if the signed receipt is not returned within 45 days.

10-407. Contractor Preparations for International Transfers Pursuant to Commercial and User Agency Sales. The contractor shall be responsible for the following preparations to facilitate international transfers:

a. Ensure that each party to be involved in the transfer is identified in the applicable contract or

agreement, and in the license application or letter request.

b. Notify the appropriate U.S. DGR when the material is ready.

c. Provide documentation or written certification by an empowered official (as defined in the ITAR) to the U.S. DGR to verify that the classified shipment is within the limitations of the pertinent export authorization or an authorized exemption to the export authorization requirements, or is within the limitations of the pertinent GCA contract.

d. Have the classified shipment ready for visual review and verification by the DGR. As a minimum this will include:

(1) Preparing the packaging materials, address labels, and receipts for review.

(2) Marking the contents with the appropriate U.S. classification or the equivalent foreign government classification, downgrading, and declassification markings, as applicable.

(3) Ensuring that shipping documents (including, as appropriate, the Shipper's Export Declaration) include the name and contact information for the CSA that validates the license or letter authorization, and the FSO or designee for the particular transfer.

(4) Sending advance notification of the shipment to the CSA, the recipient, and to the freight

forwarder, if applicable. The notification will require that the recipient confirm receipt of the shipment or provide notice to the contractor if the shipment is not received in accordance with the prescribed shipping schedule.

10-408. Transfers Pursuant to an ITAR Exemption

a. The contractor shall provide to the DGR valid documentation (i.e., license, Letter of Offer and Acceptance, or agreement) to verify the export authorization for classified technical data or certain defense articles to be transferred under an exemption to reference (v). The documentation shall include a copy of the Form DSP-83 associated with the original export authorization.

b. Classified technical data or certain defense articles to be exported pursuant to reference (v) exemptions 125.4(b)(1), 125.4(c), 125.5, 126.4(a), or 126.4(c) shall be supported by a written authorization signed by an Authorized Exemption Official or Exemption Certifying Official who has been appointed by the responsible Principal Disclosure Authority of the GCA. A copy of the authorization shall be provided by the contractor through the CSA to the Office of Defense Trade Controls.

c. Exports shall not be permitted under a Manufacturing License or Technical Assistance Agreement for which the authorization has expired.

Section 5. International Visits and Control of Foreign Nationals

10-500. General. This section describes the procedures that the United States and foreign governments have established to control international visits to their organizations and cleared contractor facilities.

10-501. International Visits

a. The contractor shall establish procedures to monitor international visits by their employees and visits or assignments to their facilities of foreign nationals to ensure that the disclosure of, and access to, export-controlled articles and related information are limited to those that are approved by an export authorization.

b. Visit authorizations shall not be used to employ or otherwise acquire the services of foreign nationals that require access to export-controlled information. An export authorization is required for such situations.

10-502. Types and Purpose of International Visits. Visit requests are necessary to make administrative arrangements and disclosure decisions, and obtain security assurances. There are three types of international visits:

a. **One-time Visits.** A visit for a single, short-term occasion (normally less than 30 days) for a specified purpose.

b. **Recurring Visits.** Intermittent, recurring visits over a specified period of time, normally up to 1 year in duration, in support of a Government-approved arrangement, such as an agreement, contract, or license. By agreement of the governments, the term of the authorization may be for the duration of the arrangement, subject to annual review, and validation.

c. **Extended Visits.** A single visit for an extended period of time, normally up to 1 year, in support of an agreement, contract, or license.

10-503. Emergency Visits. Some foreign governments will accept a visit request submitted within 7 calendar days of the proposed visit for an "emergency visit." To qualify as an emergency visit,

the visit must relate to a specific Government-approved contract, international agreement or announced request for proposal, and failure to make the visit could be reasonably expected to seriously jeopardize performance on the contract or program, or result in the loss of a contract opportunity. Emergency visits are approved only as a single, one-time visit. The requester should coordinate the emergency visit in advance with the person to be visited and ensure that the complete name, position, address, and telephone number of the person and a knowledgeable foreign government point of contact are provided in the visit request, along with the identification of the contract, agreement, or program and the justification for submission of the emergency visit request.

10-504. Requests for Recurring Visits. Recurring visit authorizations should be requested at the beginning of each program. After approval of the request, individual visits may be arranged directly with the security office of the location to be visited subject to 3 working days advance notice.

10-505. Amendments. Visit requests that have been approved or are being processed may be amended only to change, add, or delete names and change dates. Amendments requesting earlier dates than originally specified shall not be accepted. Emergency visit authorizations shall not be amended.

10-506. Visits Abroad by U.S. Contractors. Many foreign governments require the submission of a visit request for all visits to a government facility or a cleared contractor facility, even though classified information may not be involved. They also require that the requests be received a specified number of days in advance of the visit. These lead times for North Atlantic Treaty Organization (NATO) countries are in Appendix B. An export authorization must be obtained if export controlled technical data is to be disclosed or, if information to be divulged is related to a classified U.S. Government program, unless the disclosure of the information is covered by an ITAR exemption. Visit request procedures are outlined as follows:

a. **Request Format.** The visit request format is contained in Appendix B. The visit request shall be

forwarded to the security official designated by the CSA. The host for the visit should coordinate the visit in advance with appropriate government authorities who are required to approve the visit. It is the visitor's responsibility to ensure that such coordination has occurred.

b. Government Agency Programs. When contractor employees are to visit foreign government facilities or foreign contractors on U.S. Government orders in support of a government contract or agreement, a visit request shall be submitted by the contractor.

10-507. Visits by Foreign Nationals to U.S. Contractor Facilities. Requests for visits by foreign nationals to U.S. contractor facilities that will involve the disclosure of (a) classified information, (b) unclassified information related to a U.S. Government classified program, or (c) plant visits covered by Section 125.5 of reference (v) shall be processed through the sponsoring foreign government (normally the visitor's embassy) to the U.S. Government agency for approval. (NOTE: Requests for visits by foreign nationals that involve only commercial programs and related unclassified information may be submitted directly to the contractor. It is the contractor's responsibility to ensure that an export authorization is obtained, if applicable.) As described below, the U.S. government agency may approve or deny the request or decline to render a decision.

a. Government-Approved Visits. U.S. Government-approved visits constitute an exemption to the export licensing provisions of the ITAR. U.S. Government approved visits shall not be used to avoid the export licensing requirements for commercial initiatives. When the cognizant U.S. Government agency approves a visit, the notification of approval shall contain instructions on the level and scope of classified and unclassified information authorized for disclosure, as well as any limitations. Final acceptance of the visit shall be subject to the concurrence of the contractor who shall notify the U.S. Government agency when a visit is not desired.

b. Visit Request Denials. If the U.S. Government agency does not approve the disclosure of the information related to the proposed visit, it will deny the visit request. The requesting government

and the contractor to be visited shall be advised of the reason for the denial. The contractor may accept the visitor(s). However, only information that is in the public domain may be disclosed.

c. Non-Sponsorship. The U.S. Government agency will decline to render a decision on a visit request that is not in support of a U.S. Government program. A declination notice indicating that the visit is not government-approved (i.e., the visit is non-sponsored) shall be furnished to the requesting foreign government with an information copy to the U.S. contractor to be visited. A declination notice does not preclude the visit, provided the contractor has, or obtains, an export authorization for the information involved and, if classified information is involved, has been notified that the requesting foreign government has provided the required security assurance of the proposed visitor to the U.S. Government agency in the original visit request. It shall be the responsibility of the contractor to consult applicable export regulations to determine licensing requirements regarding the disclosure of export controlled information during such visits by foreign nationals.

d. Access by Foreign Visitors to Classified Information. The contractor shall establish procedures to ensure that foreign visitors are not afforded access to classified information and other export-controlled technical data except as authorized by an export license, approved visit request, or other exemption to the licensing requirements. The contractor shall not inform the foreign visitor of the scope of access authorized or of the limitations imposed by the government. Foreign visitors shall not be given custody of classified material except when they are acting as official couriers of their government and the CSA authorizes the transfer.

e. Visitor Records. The contractor shall maintain a record of foreign visitors when the visit involves access to classified information. These records shall be maintained for 1 year.

f. Visits to Subsidiaries. A visit request authorization for a visit to any element of a corporate family may be used for visits to other divisions or subsidiaries within the same corporate family provided disclosures are for the same purpose and the

information to be disclosed does not exceed the parameters of the approved visit request.

10-508. Control of Access by On-Site Foreign Nationals

a. Extended visits and assignments of foreign nationals to contractor facilities shall be authorized only when it is essential that the foreign national be at the facility pursuant to a contract or government agreement (e.g., joint venture, liaison representative to a joint or multinational program, or direct commercial sale).

b. If the foreign national will require access to export-controlled information related to, or derived from, a U.S. Government classified contract, the contractor shall obtain the written consent of the GCA before making a commitment to accept the proposed visit or assignment. A copy of the written consent shall be included with the request for export authorization, when such authorization is required.

c. The applicable CSA shall be notified in advance of all extended visits and assignments of foreign nationals to cleared contractor facilities. The notification shall include a copy of the approved visit authorization or the U.S. Government export authorization, and the TCP if applicable.

ISL 2006-02 #24 (10-508.c.). Q&A re CSA Notification of Assignment of Foreign Nationals to US Contractor Facilities (ISL 96L-1 #33).

Q: Does the requirement to notify the CSA in advance of all extended visits and assignments of foreign nationals to cleared contractor facilities apply to visits related to unclassified, non-defense, commercial programs?

A: No. This requirement applies to all foreign nationals on extended visits and assignments who are performing on classified contracts.

d. Classified U.S. and foreign government material in a U.S. contractor facility is to remain under U.S. contractor custody and control and is subject to inspection by the FSO and the CSA. This does not preclude a foreign visitor from being furnished a security container for the temporary storage of classified material, consistent with the

purpose of the visit or assignment, provided the CSA approves and responsibility for the container and its contents remains with the U.S. contractor. Exceptions to this policy may be approved on a case-by-case basis by the CSA for the storage of foreign government classified information furnished to the visitor by the visitor's government through government channels. Exceptions shall be approved in advance in writing by the CSA and agreed to by the visitor's government. The agreed procedures shall be included in the contractor's TCP, shall require the foreign nationals to provide receipts for the material, and shall include an arrangement for the CSA to ensure compliance, including provisions for the CSA to inspect and inventory the material.

ISL 2006-02 #25 (10-508.d.). Q&A re Technology Control Plan (TCP) Requirement When Foreign Nationals are Assigned to US Contractor Facilities (ISL 96L-1 #34).

Q: Is a separate Technology Control Plan required for each CSA notification?

A: A facility may have an overall Facility Technology Control Plan that can be referenced with each notification. The contractor should contact his/her local DSS Field Office to ensure that the specific controls and limitations are threat appropriate.

10-509. TCP. A TCP is required to control access by foreign nationals assigned to, or employed by, cleared contractor facilities unless the CSA determines that procedures already in place at the contractor's facility are adequate. The TCP shall contain procedures to control access for all export-controlled information. A sample of a TCP may be obtained from the CSA.

ISL 2006-02 #22 (10-307, 10-509 and Appendix C). Definitions of "Foreign National" and "U.S. Person, (ISL96L-1 #3). The NISPOM definition of a "U.S. person" is different from the definition found in the State Department's International Traffic in Arms Regulation (ITAR). Only a U.S. citizen is eligible for a personnel security clearance. Therefore, the NISPOM definition of U.S. person is an individual who is a U.S. citizen. The ITAR uses a broader definition of U.S. person based on a person's right to be hired if he or she is qualified for a job

(employment). Such employment does not establish the eligibility basis for a security clearance.

Procedures must be in place to ensure that non-U.S. citizens do not have access to U.S. classified and foreign government information. If the procedures to preclude such access are not deemed adequate by the IS Rep, a detailed Technology Control Plan will be required that includes special briefings, non-disclosure statements and more stringent access control measures.

10-510. Security and Export Control Violations Involving Foreign Nationals. Any violation of administrative security procedures or export control regulations that would subject classified information to possible compromise by foreign visitors or foreign national employees shall be reported to the CSA.

Section 6. Contractor Operations Abroad

10-600. General. This section sets forth requirements governing contractor operations abroad, including PCLs for U.S. contractor employees assigned outside the United States and their access to classified information.

10-601. Access by Contractor Employees Assigned Outside the United States.

a. Contractor employees assigned outside the United States, its possessions or territories may have access to classified information in connection with performance on a specified United States, NATO, or foreign government classified contract.

b. The assignment of an employee who is a foreign national, including intending citizens, outside the United States on programs that will involve access to classified information is prohibited and negates the basis on which an LAA may have been provided to such employee.

c. A consultant shall not be assigned outside the United States with responsibilities requiring access to classified information.

10-602. Storage, Custody, and Control of Classified Information Abroad by Employees of a U.S. Contractor.

a. The storage, custody, and control of classified information required by a U.S. contractor employee abroad is the responsibility of the U.S. Government. Therefore, the storage of classified information by contractor employees at any location abroad that is not under U.S. Government control is prohibited. The storage may be at a U.S. military facility, a U.S. Embassy or Consulate, or other location occupied by a U.S. Government organization.

b. A contractor employee may be furnished a security container to temporarily store classified material at a U.S. Government agency overseas location. The decision to permit a contractor to temporarily store classified information must be approved in writing by the senior security official for the U.S. Government host organization.

c. A contractor employee may be permitted to temporarily remove classified information from an overseas U.S. Government-controlled facility when necessary for the performance of a GCA contract or pursuant to an approved export authorization. The responsible U.S. Government security official at the U.S. Government facility shall verify that the contractor has an export authorization or other written U.S. Government approval to have the material, verify the need for the material to be removed from the facility, and brief the employee on handling procedures. In such cases, the contractor employee shall sign a receipt for the classified material. Arrangements shall also be made with the U.S. Government custodian for the return and storage of the classified material during non-duty hours. Violations of this policy shall be reported to the applicable CSA by the security office at the U.S. Government facility.

d. A contractor employee shall not store classified information at overseas divisions or subsidiaries of U.S. companies incorporated or located in a foreign country. (NOTE: The divisions or subsidiaries may possess classified information that has been transferred to the applicable foreign government through government-to-government channels pursuant to an approved export authorization or other written U.S. Government authorization. Access to this classified information at such locations by a U.S. contractor employee assigned abroad by the parent facility on a visit authorization in support of a foreign government contract or subcontract, is governed by the laws and regulations of the country in which the division or subsidiary is registered or incorporated. The division or subsidiary that has obtained the information from the foreign government shall provide the access.)

e. U.S. contractor employees assigned to foreign government or foreign contractor facilities under a direct commercial sales arrangement will be subject to the host-nation's industrial security policies.

10-603. Transmission of Classified Material to Employees Abroad. The transmission of classified material to a cleared contractor employee located outside the United States shall be through U.S. Government channels. If the material is to be used

for other than U.S. Government purposes, an export authorization is required and a copy of the authorization, validated by the DGR, shall accompany the material. The material shall be addressed to a U.S. military organization or other U.S. Government organization (e.g., an embassy). The U.S. government organization abroad shall be responsible for custody and control of the material.

10-604. Security Briefings. An employee being assigned outside the United States shall be briefed on the security requirements of his or her assignment, including the handling, disclosure, and storage of classified information overseas.

Section 7. NATO Information Security Requirements

10-700. General. This section provides the security requirements needed to comply with the procedures established by the U.S. Security Authority for NATO (USSAN) for safeguarding NATO information provided to U.S. industry.

10-701. Classification Levels. NATO has the following levels of security classification: COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR). Another marking, ATOMAL, is applied to U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA and United Kingdom Atomic information that has been released to NATO. ATOMAL information is marked COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA).

10-702. NATO RESTRICTED. NATO RESTRICTED does not correspond to an equivalent U.S. classification. NATO RESTRICTED does not require a PCL for access. An FCL is not required if the only information to which the company will have access is NATO RESTRICTED. IS handling only NATO RESTRICTED information do not require certification or accreditation. NATO RESTRICTED information may be included in U.S. unclassified documents. The U.S. document must be marked, "THIS DOCUMENT CONTAINS NATO RESTRICTED INFORMATION." NATO RESTRICTED material may be stored in locked filing cabinets, bookcases, desks, or other similar locked containers that will deter unauthorized access.

ISL 2006-01 #21 (10-702). The requirement to protect NATO RESTRICTED information as U.S. classified has been eliminated. For access to NATO RESTRICTED, no FCL is required for the company, PCLs are not required for personnel, and neither certification nor accreditation are required for information systems. However, the information shall not be disclosed to anyone except personnel who require access in connection with the contract.

10-703. NATO Contracts. NATO contracts involving NATO-unique systems, programs, or operations are awarded by a NATO Production and Logistics Organization (NPLO), a designated NATO

Management Agency, the NATO Research Staff, or a NATO Command. In the case of NATO infrastructure projects (e.g., airfields, communications), the NATO contract is awarded by a contracting agency or prime contractor of the NATO nation responsible for the infrastructure project.

10-704. NATO Facility Security Clearance Certificate. A NATO Facility Security Clearance Certificate (FSCC) is required for a contractor to negotiate or perform on a NATO classified contract. A U.S. facility qualifies for a NATO FSCC if it has an equivalent U.S. FCL and its personnel have been briefed on NATO procedures. The CSA shall provide the NATO FSCC to the requesting activity. A NATO FSCC is not required for GCA contracts involving access to NATO classified information.

10-705. PCL Requirements. Access to NATO classified information requires a final PCL at the equivalent level.

10-706. NATO Briefings. Before having access to NATO classified information, employees shall be given a NATO security briefing that covers the requirements of this section and the consequences of negligent handling of NATO classified information. The FSO shall be initially briefed by a representative of the CSA. Annual refresher briefings shall also be conducted. When access to NATO classified information is no longer required, the employee shall be debriefed. The employee shall sign a certificate stating that they have been briefed or debriefed, as applicable, and acknowledge their responsibility for safeguarding NATO information. Certificates shall be maintained for 2 years for NATO SECRET and CONFIDENTIAL, and 3 years for COSMIC TOP SECRET and all ATOMAL information. The contractor shall maintain a record of all NATO briefings and debriefings in the CSA-designated database.

10-707. Access to NATO Classified Information by Foreign Nationals. Foreign nationals of non-NATO nations may have access to NATO classified information only with the consent of the NATO Office of Security and the contracting activity. Requests shall be submitted to the Central U.S.

Registry (CUSR). Access to NATO classified information may be permitted for citizens of NATO member nations, provided a NATO security clearance certificate is provided by their government and they have been briefed.

10-708. Subcontracting for NATO Contracts. The contractor shall obtain prior written approval from the NATO contracting activity and a NATO FSCC must be issued prior to awarding the subcontract. The request for approval will be forwarded through the CSA.

10-709. Preparing and Marking NATO Documents. All classified documents created by a U.S. contractor shall be portion-marked. Any portion extracted from a NATO document that is not portion marked, must be assigned the classification that is assigned to the NATO document.

a. All U.S.-originated NATO classified documents shall bear an assigned reference number and date on the first page. The reference numbers shall be assigned as follows:

(1) The first element shall be the abbreviation for the name of the contractor facility.

(2) The second element shall be the abbreviation for the overall classification followed by a hyphen and the 4-digit sequence number for the document within that classification that has been generated for the applicable calendar year.

(3) The third element shall be the year; e.g., MM/NS-0013/93.

b. COSMIC TOP SECRET, NATO SECRET, and ATOMAL documents shall bear the reference number on each page and a copy number on the cover or first page. Copies of NATO documents shall be serially numbered. Pages shall be numbered. The first page or index or table of contents shall include a list, including page numbers, of all Annexes and Appendices. The total number of pages shall be stated on the first page. All Annexes or Appendices will include the date of the original document and the purpose of the new text (addition or substitution) on the first page.

c. One of the following markings shall be applied to NATO documents that contain ATOMAL information:

(1) "This document contains U.S. ATOMIC Information (RESTRICTED DATA or FORMERLY RESTRICTED DATA) made available pursuant to the NATO Agreement for Cooperation Regarding ATOMIC Information, dated 18 June 1964, and will be safeguarded accordingly."

(2) "This document contains UK ATOMIC Information. This information is released to NATO including its military and civilian agencies and member states on condition that it will not be released by the recipient organization to any other organization or government or national of another country or member of any other organization without prior permission from H.M. Government in the United Kingdom."

d. Working papers shall be retained only until a final product is produced.

10-710. Classification Guidance. Classification guidance shall be in the form of a NATO security aspects letter and a security requirements checklist for NATO contracts, or a Contract Security Classification Specification. If adequate classification guidance is not received, the contractor shall contact the CSA for assistance. NATO classified documents and NATO information in other documents shall not be declassified or downgraded without the prior written consent of the originating activity. Recommendations concerning the declassification or downgrading of NATO classified information shall be forwarded to the CUSR.

10-711. Further Distribution. The contractor shall not release or disclose NATO classified information to a third party or outside the contractor's facility for any purpose without the prior written approval of the contracting agency.

10-712. Storage of NATO Documents. NATO classified documents shall be stored as prescribed for U.S. documents of an equivalent classification level, except as follows:

a. NATO classified documents shall not be commingled with other documents.

b. Combinations for containers used to store NATO classified information shall be changed annually. The combination also shall be changed when an individual with access to the container departs or no longer requires access to the container, and if the combination is suspected of being compromised.

c. When the combination is recorded it shall be marked with the highest classification level of documents stored in the container as well as to indicate the level and type of NATO documents in the container. The combination record must be logged and controlled in the same manner as NATO classified documents.

10-713. International Transmission. NATO has a registry system for the receipt and distribution of NATO documents within each NATO member nation. The central distribution point for the U.S. is the CUSR located in the Pentagon. The CUSR establishes subregistries at U.S. Government organizations for further distribution and control of NATO documents. Subregistries may establish control points at contractor facilities. COSMIC TOP SECRET, NATO SECRET, and all ATOMAL documents shall be transferred through the registry system. NATO CONFIDENTIAL documents provided as part of NATO infrastructure contracts shall be transmitted via government channels in compliance with Section 4 of this Chapter.

10-714. Handcarrying. NATO SECRET and NATO CONFIDENTIAL documents may be handcarried across international borders if authorized by the GCA. The courier shall be issued a NATO Courier Certificate by the CSA. When handcarrying is authorized, the documents shall be delivered to a U.S. organization at NATO, which shall transfer them to the intended NATO recipient.

10-715. Reproduction. Reproductions of COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL information shall be performed by the responsible Registry. The reproduction of NATO SECRET, and CONFIDENTIAL documents may be authorized to meet contractual requirements unless reproduction is prohibited by the contracting entity. Copies of COSMIC TOP SECRET, NATO SECRET, and ATOMAL documents shall be serially numbered

and controlled and accounted for in the same manner as the original.

10-716. Disposition. Generally, all NATO classified documents shall be returned to the contracting activity that provided them on completion of the contract. Documents provided in connection with an invitation to bid also shall be returned immediately if the bid is not accepted or submitted. NATO classified documents may also be destroyed when permitted. COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL documents shall be destroyed by the Registry that provided the documents. Destruction certificates are required for all NATO classified documents except NATO CONFIDENTIAL. The destruction of COSMIC TOP SECRET, NATO SECRET and all ATOMAL documents must be witnessed.

10-717. Accountability Records. Logs, receipts, and destruction certificates are required for NATO classified information, as described below. Records for NATO documents shall be maintained separately from records of non-NATO documents. COSMIC TOP SECRET and all ATOMAL documents shall be recorded on logs maintained separately from other NATO logs and shall be assigned unique serial control numbers. Additionally, disclosure records bearing the name and signature of each person who has access are required for all COSMIC TOP SECRET, COSMIC TOP SECRET ATOMAL, and all other ATOMAL or NATO classified documents to which special access limitations have been applied.

a. Minimum identifying data on logs, receipts, and destruction certificates shall include the NATO reference number, short title, date of the document, classification, and serial copy numbers. Logs shall reflect the short title, unclassified subject, and distribution of the documents.

b. Receipts are required for all NATO classified documents except NATO CONFIDENTIAL.

c. Inventories shall be conducted annually of all COSMIC TOP SECRET, NATO SECRET, and all ATOMAL documents.

d. Records shall be retained for 10 years for COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL documents and 5 years for

NATO SECRET, NATO SECRET ATOMAL, NATO CONFIDENTIAL, and NATO CONFIDENTIAL ATOMAL documents.

10-718. Security Violations and Loss, Compromise, or Possible Compromise. The contractor shall immediately report the loss, compromise, or suspected loss or compromise, as well as any other security violations involving NATO classified information to the CSA.

10-719. Extracting from NATO Documents. Permission to extract from a COSMIC TOP SECRET or ATOMAL document shall be obtained from the CUSR.

a. If extracts of NATO information are included in a U.S. document prepared for a non-NATO contract, the document shall be marked with U.S. classification markings. The caveat, "THIS DOCUMENT CONTAINS NATO (level of classification) INFORMATION" also shall be marked on the front cover or first page of the document. Additionally, each paragraph or portion containing the NATO information shall be marked with the appropriate NATO classification, abbreviated in parentheses (e.g., NS) preceding the portion or paragraph. The "Declassify on" line of the document shall show "Source marked OADR" and the date of origin of the most recent source document unless the original NATO document shows a specific date for declassification.

b. The declassification or downgrading of NATO information in a U.S. document requires the approval of the originating NATO activity. Requests shall be submitted to the CUSR for NATO contracts, through the GCA for U.S. contracts, and through the CSA for non-NATO contracts awarded by a NATO member nation.

10-720. Release of U.S. Information to NATO.

a. Release of U.S. classified or export-controlled information to NATO requires an export authorization or other written disclosure authorization. When a document containing U.S. classified information is being prepared for NATO, the appropriate NATO classification markings shall be applied to the document. Documents containing U.S. classified information and U.S. classified

documents that are authorized for release to NATO shall be marked on the cover or first page "THIS DOCUMENT CONTAINS U.S. CLASSIFIED INFORMATION. THE INFORMATION IN THIS DOCUMENT HAS BEEN AUTHORIZED FOR RELEASE TO (cite the NATO organization) BY (cite the applicable license or other written authority)." The CSA shall provide transmission instructions to the contractor. The material shall be addressed to a U.S. organization at NATO, which shall then place the material into NATO security channels. The material shall be accompanied by a letter to the U.S. organization that provides transfer instructions and assurances that the material has been authorized for release to NATO. The inner wrapper shall be addressed to the intended NATO recipient. Material to be sent to NATO via mail shall be routed through the U.S. Postal Service and U.S. military postal channels to the U.S. organization that will make the transfer.

b. A record shall be maintained that identifies the originator and source of classified information that are used in the preparation of documents for release to NATO. The record shall be provided with any request for release authorization.

10-721. Visits. NATO visits are visits by personnel representing a NATO entity and relating to NATO contracts and programs. NATO visits shall be handled in accordance with the requirements in Section 5 of this chapter. A NATO Certificate of Security Clearance will be included with the visit request.

a. NPLO and NATO Industrial Advisory Group (NIAG) Recurring Visits. NATO has established special procedures for recurring visits involving contractors, government departments and agencies, and NATO commands and agencies that are participating in a NPLO or NIAG contract or program. The NATO Management Office or Agency responsible for the NPLO program will prepare a list of the Government and contractor facilities participating in the program. For NIAG programs, the list will be prepared by the responsible NATO staff element. The list will be forwarded to the appropriate clearance agency of the participating nations, which will forward it to the participating contractor.

b. **Visitor Record.** The contractor shall maintain a record of NATO visits including those by U.S. personnel assigned to NATO. The records shall be maintained for 3 years.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 8. Transfers of Defense Articles to the United Kingdom without a License or Other Written Authorization

10-800 General. On June 21, 2007, the U.S. signed the Defense Trade Cooperation Treaty between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland Concerning Defense Trade Cooperation (U.S.-U.K. Treaty). The U.S.-U.K. Treaty entered into force on April 13, 2012. The U.S.-U.K. Treaty provides a comprehensive framework for exports and transfers to the UK of certain classified and unclassified defense articles without a license or other written authorization. Reference (v) has been amended to implement the U.S.-U.K. Treaty. Amendments included a new exemption in part 126.17 Supplement No. 1 to part 126 of reference (v), which identifies those defense articles exempt from the scope of reference (v). This exemption applies to contractors registered with the State Department, Directorate of Defense Trade Controls (DDTC), and eligible to export defense articles.

10-801 Defense Articles. Defense articles fall under the scope of the U.S.-U.K. Treaty when they are in support of:

- a. U.S. and U.K. combined military or counter-terrorism operations;
- b. U.S. and U.K. cooperative security and defense research, development, production, and support programs;
- c. Mutually agreed specific security and defense projects where the Government of the U.K. is the end-user; or
- d. U.S. Government end-use.

10-802. Marking Requirements. Contractors are required to mark defense articles that fall under the scope of the treaty prior to transferring from the U.S. to the U.K. as follows:

- a. Classified U.S. Defense Articles shall be marked:

CLASSIFICATION LEVEL USML//REL
USA AND GBR TREATY COMMUNITY//

For example, for defense articles classified SECRET, the marking shall be "SECRET USML//REL USA AND GBR TREATY COMMUNITY//"

- b. All other standard classification markings in accordance with Chapter 4, Section 2 of this Manual shall apply.

- c. Unclassified U.S. defense articles shall be marked:

//RESTRICTED USML//REL USA AND
GBR TREATY COMMUNITY//

- d. When defense articles are returned from the U.K. to the U.S., any defense articles marked as RESTRICTED in this manner purely for the purposes of the U.S.-U.K. Treaty shall be considered to be unclassified and such marking shall be removed.

10-803 Transfers.

- a. All Defense Articles that fall under the scope of the U.S.-U.K. Treaty must be transferred from the U.S. point of embarkation through channels approved by both the U.S. and the U.K.

- b. For transfers of defense articles as freight, the contractor shall prepare a transportation plan. For transfer of classified U.S. defense articles, a freight forwarder must have a valid facility security clearance (FCL) 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.

10-804 Records. Contractors shall maintain records of exports, transfers, re-exports, or re-transfers of defense articles subject to the U.S.-U.K. Treaty for a period of 5 years. Records shall be made available to DSS upon request. The records shall contain the following information required by 126.17(l)(1) of reference (v):

- a. Port of entry or exit.
- b. Date and time of export or import.

- c. Method of export or import.
- d. Commodity code and description of the commodity, including technical data
- e. Value of export.
- f. Reference (v) and justification for export under the Treaty.
- g. End-user or end-use.
- h. Identification of all U.S. and foreign parties to the transaction.
- i. How export was marked.
- j. Security classification of the export.
- k. All written correspondence with the U.S. Government on the export.
- l. All information relating to political contributions, fees, or commissions furnished or obtained, offered, solicited, or agreed upon, as outlined in part 126.17(m) of reference (v).
- m. Purchase order, contract, or letter of intent.
- n. Technical data actually exported.
- o. The Internal Transaction Number for the Electronic Export Information filing in the Automated Export System.
- p. All shipping documentation (including, but not limited to, the airway bill, bill of lading, packing list, delivery verification, and invoice).
- q. Statement of Registration (Form DS-2032).

ISL 2013-03. Transfers of Defense Articles to Australia without a License or Other Written Authorization

The U.S. Government signed a treaty with the Government of Australia Concerning Defense Trade Cooperation on September 5, 2007. This treaty provides a comprehensive framework for certain exports from the United States to Australia and vice versa, as well as certain transfers within and between the United States (U.S.) and Australia (AUS) of certain classified and unclassified Defense Articles without a license or other written authorization. This Industrial Security Letter (ISL) promulgates updated guidance for information and interpretation of existing paragraphs in Chapters 4 and 10 of the National Industrial Security Program Operating Manual (NISPOM) based on the requirements of that Treaty, for exports and transfers of Defense Articles to Australia. Specific changes to Chapters 4 and 10 of the NISPOM will be published shortly.

Part 126 of the International Traffic in Arms Regulations (ITAR) has been amended to add a new exemption in §126.16 to implement the Treaty, and to revise Supplement No. 1 to Part 126, which identifies those Defense Articles exempt from the scope of §126.16, as well as §126.5 and §126.17. The guidance provided in this article applies to contractors registered with the Department of State,

Directorate of Defense Trade Controls (DDTC) and who are eligible to export.

Definitions:

Defense Articles are those articles, services, and related technical data, including software, in tangible or intangible form, listed on the United States Munitions List (USML). Defense Articles exempt from the scope of §126.16 of the ITAR are identified in Supplement No. 1 to Part 126 of the ITAR.

Defense Articles fall under the scope of §126.16 when they are in support of:

1. U.S. and AUS combined military or counter-terrorism operations;
2. U.S. and AUS cooperative security and defense research, development, production, and support programs;
3. Mutually agreed specific security and defense projects where the Government of Australia is the end-user; or
4. U.S. Government end-use.

A listing of approved operations, programs, projects and end-uses is available on DDTC's website under the Treaty tab at (<http://pmddtc.state.gov/>).

AUS Community consists of the Government of Australia entities and Australian non-governmental facilities identified on the DDTC website (<http://pmddtc.state.gov/>) at the time of export or transfer.

Marking:

Contractors are required to mark Defense Articles that fall under the scope of the Treaty prior to transferring from the United States to Australia as follows:

Treaty with the Government of Australia

Classified U.S. Defense Articles will be marked:

//CLASSIFICATION LEVEL USML//REL AUS AND USA TREATY COMMUNITY//

For example, for Defense Articles classified SECRET, the marking will be
“//SECRET USML//REL AUS AND USA TREATY COMMUNITY//”

All other standard classification markings in accordance with NISPOM Chapter 4, Section 2 will apply.

Unclassified U.S. Defense Articles will be marked
//RESTRICTED USML//REL AUS AND USA TREATY COMMUNITY//

When U.S.-origin Defense Articles are returned to a member of the United States, any Defense Articles marked or identified as RESTRICTED, for the purposes of the Treaty, will be considered UNCLASSIFIED and the marking or identification will be removed.

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."

Defense articles (as defined in ITAR §120.6) (other than technical data) shall be individually labeled with the appropriate identification; or, where such labeling is impracticable (e.g., propellants, chemicals), shall be accompanied by documentation (such as contracts or invoices) clearly associating the defense articles with the appropriate markings;

Technical data (as defined in ITAR §120.10) (including data packages, technical papers, manuals, presentations, specifications, guides and reports), regardless of media or means of transmission (i.e., physical, oral, or electronic), shall be individually labeled with the appropriate identification detailed; or, where such labeling is impracticable shall be accompanied by documentation (such as contracts or invoices) or oral notification clearly associating the technical data with the appropriate markings; and

Defense services (as defined in ITAR §120.9) shall be accompanied by documentation (contracts, invoices, shipping bills, or bills of lading) clearly labeled with the appropriate identification.

Transfers:

In accordance with NISPOM Chapter 10, Section 4, 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 United States and Australia.

For transfers of Defense Articles as freight, the contractor will prepare a transportation plan. For transfers of classified U.S. Defense Articles, a freight forwarder must have a valid facility security clearance (FCL) 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.

Records:

Contractors will maintain records of exports and transfers of Defense Articles falling under the scope of the Treaty for a minimum of five years. Records will be made available to the Defense Security Service (DSS) upon request. The records will contain the following information (as required by ITAR §126.16(l)(1)):

1. Port of entry/exit;
2. Date of export/import;
3. Method of export/import;
4. Commodity code and description of the commodity, including technical data;
5. Value of export;
6. Reference to ITAR §126.16, and justification for export under the Treaty;
7. End-user/end-use;
8. Identification of all U.S. and foreign parties to the transaction;
9. How export was marked;
10. Security classification of the export;
11. All written correspondence with the U.S. Government on the export;
12. All information relating to political contributions, fees, or commissions furnished or obtained, offered, solicited, or agreed upon as outlined in ITAR §126.16(m);
13. Purchase order or contract;
14. Technical data actually exported;
15. The Internal Transaction Number for the Electronic Export Information filing in the Automated Export System;
16. All shipping documentation (including, but not limited to the airway bill, bill of lading, packing list, delivery verification, and invoice); and
17. Statement of Registration (Form DS-2032).

CHAPTER 11

Miscellaneous Information

Section 1. TEMPEST

11-100. General. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment.

11-101. TEMPEST Requirements.

a. TEMPEST countermeasures will be applied only in proportion to the threat of exploitation and the resulting damage to the national security should the information be intercepted and analyzed by a foreign intelligence organization. It is the responsibility of the GCA to identify in writing what TEMPEST countermeasures may be required. The GCA will identify any TEMPEST requirements within the United States to the CSA for approval prior to imposing requirements for TEMPEST countermeasures on contractors. Contractors may not impose TEMPEST countermeasures upon their subcontractors without GCA and CSA approval.

b. The government is responsible for performing threat assessment and vulnerability studies when it is

determined that classified information may be exposed to TEMPEST collection.

c. Contractors will assist the GCA in conducting threat and vulnerability surveys by providing the following information upon request:

(1) The specific classification and special categories of material to be processed/handled by electronic means.

(2) The specific location where classified processing will be performed.

(3) The name, address, title, and contact information for a point-of-contact at the facility where processing will occur.

11-102. Cost. All costs associated with applying TEMPEST countermeasures, when such countermeasures are imposed upon the contractor by a GCA, shall be recoverable by direct charge to the applicable contract. The GCA should provide TEMPEST shielding and shielded equipments as government-furnished equipment (GFE) when such extreme countermeasures are deemed essential to the protection of the information being processed.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

Section 2. Defense Technical Information Center (DTIC)

11-200. General. The Department of Defense operates certain activities to assist individuals and organizations in gaining access to scientific and technical information describing planned or on-going research, development, technical and engineering (RDT&E) efforts of the Department of Defense. DTIC is the central point within the Department of Defense for acquiring, storing, retrieving, and disseminating scientific and technical information to support the management and conduct of DoD RDT&E and study programs.

11-201. User Community. DTIC services are available to the Department of Defense and its contractors, as well as to other U.S. Government organizations and their contractors. Contractors may also become eligible for services under the Defense Potential Contractors Program.

11-202. Registration Process. All users are required to register for service. Registration, which is free, generally involves completing two forms which are available from DTIC as part of a registration kit.

a. DD Form 1540, Registration for Scientific and Technical Information Services. This form shall be completed for each contract that authorizes use of DTIC services. This authorization is included in the Contract Security Classification Specification. The DD Form 1540 is submitted to DTIC through the sponsoring GCA for certification and approval. If a subcontract is involved, the DD Form 1540 is submitted through the prime contractor. The DD Form 1540 remains in force until completion of the classified contract or subcontract.

b. DD Form 2345, Militarily Critical Technical Data Agreement. Qualified contractors are eligible for access to militarily critical technical data after certification with Defense Logistics Services Center (DLSC) by completing the DD Form 2345. This DLSC certification is supplementary to registration with the DTIC. Upon certification with DLSC, the user also may be eligible for access to unclassified, militarily critical technical data from other DoD sources.

11-203. Safeguarding Requirements. Classified information acquired from DTIC shall be

safeguarded according to the requirements of this Manual and with any restrictions that are marked on the material itself. The specific contract number that authorized contractor access to the information shall be placed on each classified document. When the contract to which the DD Form 1540 applies is completed or terminated, the contractor shall either destroy or request retention for the material.

11-204. DTIC Downgrading or Declassification Notices. DTIC re-marks downgraded or declassified paper documents only on the front and back covers and the title, first, and back pages. It is the responsibility of the recipient to complete any remarking required. Documents originally marked under the provisions of previous E.O.s may contain pages that do not bear any classification markings. Before extracting or reproducing the information from these pages, contractors should direct any questions they may have to the originator of the document.

11-205. Questions Concerning Reference Material. Most material made available to contractors by DTIC and other distribution agencies is reference material. Therefore, the GCA that authorized the services of DTIC under a specific contract may not be in a position to provide the contractor with classification guidance for the reference material. Classification jurisdiction always is the responsibility of the originating agency, or its successor. Classification jurisdiction is not necessarily the responsibility of the authorizing GCA. When a contractor needs assistance in identifying the responsible department or agency for classification guidance for reference material the CSA should be consulted.

11-206. Subcontracts. If a contractor awards a subcontract that authorizes the subcontractor to use the services of DTIC and is expected to require access only to classified reference material, the Contract Security Classification Specification issued to the subcontractor shall show the highest category of classification required. The Contract Security Classification Specification will have a statement similar to the following: "Information extracted from classified reference material shall be classified according to the markings on such material. The DD

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

Form 1540 prepared under this subcontract shall be
forwarded through (name of prime contractor)."

Section 3. Independent Research and Development (IR&D) Efforts

11-300. General. This section provides special procedures and requirements necessary for safeguarding classified information when it is incorporated in contractors' IR&D efforts.

11-301. Information Generated Under an IR&D Effort that Incorporates Classified Information. Under reference (b) information that is in substance the same as information currently classified requires a derivative classification. Therefore, information in a contractor's IR&D effort will require a derivative classification.

11-302. Classification Guidance. The releasing contractor may extract guidance appropriate for the IR&D effort from:

- a. An existing Contract Security Classification Specification that was previously furnished by a GCA in connection with performance of a classified contract;
- b. A final Contract Security Classification Specification that was issued in connection with retention of classified documents under a completed contract;
- c. A security classification guide obtained from DTIC; or
- d. A classified source document

NOTE: The Department of Defense "Index of Security Classification Guides" and many of the listed security classification guides are available to contractors who are registered with the DTIC. Contractors are encouraged to use the Index and the listed guides to obtain up-to-date security guidance for the classified information involved when developing guidance appropriate for their IR&D efforts.

11-303. Preparation of Security Guidance. Contractors shall use the Contract Security Classification Specification to provide security guidance for the classified information released in their IR&D efforts.

11-304. Retention of Classified Documents Generated Under IR&D Efforts. Contractors may retain the classified documents that were generated in connection with their classified IR&D efforts for the duration of their FCL provided they have proper storage capability. Documents shall be clearly identified as "IR&D DOCUMENTS." A contractor's facility clearance will not be continued solely for the purpose of retention of classified IR&D documents without specific retention authorization from the GCA that has jurisdiction over the classified information contained in such documents. Contractors shall establish procedures for review of their IR&D documents on a recurring basis to reduce their classified inventory to the minimum necessary.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

APPENDIX A: Cognizant Security Office Information

(Note: Appendix A was not included in Change 1, dated March 28, 2013. The following was taken from the NISPOM, dated February 28, 2006.)

Department of Defense

DSS is headquartered in Northern Virginia. The field organization structure consists of four regions. Each region is comprised of Field Offices that employ Industrial Security Representatives to provide security oversight, consultation and assistance to over 11,000 contractors. Field Offices are located throughout the United States. Refer to the DSS website (www.dss.mil) for a listing of office locations and areas of responsibility.

Verification of Facility Clearance and Safeguarding:
www.dss.mil

Other questions:
DoD Security Services Center
Phone: 1-888-282-7682

Department of Energy

DOE designates the DOE Field Office Safeguards and Security Divisions, listed below, as CSO, Clearance Agency, CVA, Adjudicative Authority, and PCL and FCL databases for their contractors.

Office of Headquarters Security Operations
SO-30/Germantown Building
U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, D.C. 20585-1290
(301) 903-4175

U.S. Department of Energy
Albuquerque Operations Office
Pennsylvania & H Street,
Kirtland Air Force Base
Albuquerque, NM 87116
(505) 845-4154

U.S. Department of Energy
Chicago Regional Office
One South Wacker Drive, Suite 2380
Chicago, IL 60606-4616
(630) 252-2000

U.S. Department of Energy
Idaho Operations Office
850 Energy Drive
Idaho Falls, ID 83401
(208) 526-1322

U.S. Department of Energy
Nevada Operations Office
232 Energy Way
North Las Vegas, NV 89030-4199
(702) 295-1000

U.S. Department of Energy
Oak Ridge Operations Office
200 Administration Road
Oak Ridge, TN 37831
(865) 576-2140

U.S. Department of Energy
Pittsburgh Naval Reactors
814 Pittsburgh McKeesport Boulevard
West Mifflin, PA 15122-0109
(412) 476-5000

U.S. Department of Energy
Richland Operations Office
825 Jadwin Avenue
P.O. Box 550
Richland, WA 99352
(509) 376-7411

U.S. Department of Energy
Savannah River Operations Office
Road 1A
Aiken, SC 29801
(803) 725-6211

U.S. Department of Energy
Schenectady Naval Reactors Office
U.S. DOE Building MS Warehouse
2401 River Road
Schenectady, NY 12309
(518) 395-4000

With regard to International Affairs and Industrial Security International, the DOE designates:

Office of International Safeguards and Security
SO-20.3/Germantown Building
U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, D.C. 20585-1290
(301) 903-2910

Central Intelligence Agency

The CIA designates the procedure listed below, for CSO, Clearance Agency, CVA, Adjudicative Authority, and PCL and FCL databases for their contractors.

Contact the assigned Contract Officer's Security Representative (COSR) Central Intelligence Agency
Washington, DC 20505

Nuclear Regulatory Commission

The NRC designates the office listed below as the CSO, Adjudicative Authority, International Affairs

Office, PCL and FCL databases, and the Office of Industrial Security International for their contractors.

U.S. Nuclear Regulatory Commission
ATTN: Director of Security
Washington, DC 20555
(301) 415-8100

The NRC designates the offices listed below as the Clearance Agency and Central Verification Agency for their contractors.

Clearance Agency:
U.S. Nuclear Regulatory Commission
ATTN: Director of Security Personnel Security Branch
Washington D.C. 20555
(301) 415-7043

Central Verification Agency:
U.S. Nuclear Regulatory Commission
ATTN: Director of Security Facilities Security Branch
Washington, D.C. 20555
(301) 415-7407

APPENDIX B: International Visits

(Note: Appendix B was not included in Change 1, dated March 28, 2013. The following was taken from the NISPOM, dated February 28, 2006.)

Standard Request for Visit Format (RFV)

This appendix contains the instructions for the completion of a Request for Visit (RFV) for international visits. The visit request must be submitted through the FSO to the applicable clearance agency. The RFV format below, will be used for all requests for international visits as follows:

- (1) A separate request must be submitted for each program, project, or contract.
- (2) A separate request must be submitted for each country to be visited.
- (3) Subject to Government Agency restrictions, multiple locations may be listed for each country provided each location is involved in the same program, project, or contract.
- (4) The RFV may be locally produced on a form or form letter provided the specified format is followed. Information given to answer each data element must be typed or printed in block letters so that it is legible.

1. GENERAL INSTRUCTION

- 1.1. The RFV is an important document and must be completed without misstatement or omission. Failure to provide all requested information will delay the processing of the request.
- 1.2. The RFV should be used for a "one-time visit" and/or "recurring visits" and/or an "emergency visit" during a certain period of time not to exceed one year.
- 1.3. The RFV should be marked to identify which type of information or subject will be involved:
 - 1.3.1. Unclassified/RESTRICTED information without access to information or areas classified CONFIDENTIAL or above.
 - 1.3.2. Information or areas classified CONFIDENTIAL or above.
- 1.4. This RFV should be hand written in block letters or typed. Processing of the RFV in an IS is allowed provided that the original form and content are consistent.
- 1.5. **Submitting Terms and Country Codes.**

The RFV should be in the possession of the requesting National Security Authority/Designated Security Authority (NSA/DSA) the number of working days prior to the visit as follows:

Country to be visited	2 letter-code	Working days (if different from lead times as shown in Section I)
Austria	AT	20
Belgium	BE	20
Canada	CA	20
Czech Republic	CZ	20
Denmark	DA	7
France	FR	15
Germany	GE	20
Hungary	HU	20
Italy	IT	20
Luxembourg	LU	14
Netherlands	NL	10
Norway	NO	10
Portugal	PO	21
Poland	PL	25
Spain	SP	20
Sweden	SE	15
Switzerland	SZ	20
Turkey	TU	21
United Kingdom	UK	15
United States	US	21

- 1.6. The completed RFV should be sent to the following national agency/address that will process the request (to be inserted by issuing NSA/DSA):

Name of Agency:	
Address:	
Telefax no:	

DETAILED INSTRUCTIONS FOR COMPLETION OF REQUEST FOR VISIT

(The application has to be submitted in English only)

These detailed instructions are guidance for the visitors who complete the RFV in the case of one-time visits or by the agency or facility security officer in case of recurring visits in the framework of approved programs or projects. Since this RFV-format is designed for manual as well as for automated use it is required that a corresponding distinction is made in the completion of some items. When this distinction is applicable reference is made in the text of the item under "Remark(s)".

Heading: In case of a manual application mark the appropriate box in left, middle and right column.

HEADING	Check boxes for visit type, information or access type, and whether or not there are annexes to the RFV.
1. ADMINISTRATIVE DATA	Do not fill in (to be completed by requesting Embassy).
2. REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY.	Mention full name and postal address. Include city, state, postal zone as applicable.
3. GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED	<p>Mention full name and postal address. Include city, state, postal zone, telex or fax number, telephone number and e-mail. Mention the name and telephone/fax numbers and e-mail of your main point of contact or the person with whom you have made the appointment for the visit.</p> <p><u>Remarks:</u> 1) Mentioning the correct postal zone (zip code) is very important because there can be different facilities of the same company.</p> <p>2) In case of a manual application, Annex 1 can be used when two or more agencies or facilities have to be visited in the framework of the same subject. When an Annex is used item 3 should state: "SEE ANNEX 1, NUMBER OF AGENCIES/FAC.:" (state number of agencies/ facilities).</p> <p>3) For visits to the United States one request for each agency/facility to be visited should be filled in.</p>
4. DATES OF VISIT	Mention the actual date or period (date-to-date) of the visit by "day- month-year". If applicable, place an alternate date or period in brackets.
5. TYPE OF VISIT	Mark one item of each column as indicated. Government initiative will be specified only if the visit is in support of an authorized government program, which must be fully described in item 8.
6. SUBJECT TO BE DISCUSSED / JUSTIFICATION	<p>Give a brief description of the subject(s) motivating the visit. Do not use unexplained abbreviations.</p> <p><u>Remarks:</u> 1) In case of a recurring visit this item should state "Recurring Visits" as the first words in the data element(e.g. Recurring Visits to discuss_____)</p>

	2) It is strongly advised to repeat the subject to be discussed and or the justification of the visit in the language of the receiving country.
7. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED	TOP SECRET (TS) SECRET (S) CONFIDENTIAL (C) RESTRICTED (R) UNCLASSIFIED (U) – As applicable
8. IS THE VISIT PERTINENT TO: Specific equipment or weapon system Foreign military sales or export license A Program or Agreement A defense acquisition process Other	Mark the appropriate line yes (Y) and specify the full name of the government project/program, FMS-case etc., or request for proposal or tender offer using commonly used abbreviations only
9. PARTICULARS OF VISITOR	<p><u>NAME</u>: Title (Mr. Dr. COL), family name, first forename in full, middle initial(s), and suffix (Jr., PhD, etc.). Family name and first forename are mandatory fields.</p> <p><u>DOB</u>: date of birth (day-month-year)</p> <p><u>POB</u>: place of birth (city-state-country)</p> <p><u>SC</u>: actual security clearance status, e.g., TS, S, C. Indicate NATO clearance (CTS, NS, NC) if the visit is related to NATO business.</p> <p><u>ID-PP</u>: enter the number of identification card or passport, as required by host government.</p> <p><u>NAT</u>: enter nationality and/or citizenship in 2-letter-code in accordance with the General Instructions paragraph 1.4.</p> <p><u>POSITION</u>: Mention the position the visitor holds in the organization (e.g., director, product manager, etc.)</p> <p><u>COMPANY/AGENCY</u>: Mention the name of the government agency or industrial facility that the visitor represents (if different from item 2).</p> <p>[Remark: when more than 2 visitors are involved in the visit, Annex 2 should be used. In that case item no. 9 should state "SEE ANNEX 2, NUMBER OF VISITORS:" (state the number of visitors)].</p>
10. THE SECURITY OFFICER OF THE REQUESTING AGENCY	This items requires the name, telephone, facsimile numbers and e-mail of the requesting facility security officer
11. CERTIFICATION OF SECURITY CLEARANCE	<u>DO NOT FILL IN</u> (to be completed by government certifying authority only if access to information or to areas classified CONFIDENTIAL or above will be involved unless otherwise required by bi-lateral agreements.)

	<p>Note for the certifying authority:</p> <p>a. Mention name, address, telephone, facsimile numbers and e-mail (can be pre-printed).</p> <p>b. This item should be signed and eventually stamped, as applicable.</p> <p>c. If the certifying authority corresponds with the requesting National Security Authority enter: "See item 12".</p> <p><u>Remark:</u> Item 11 and 12 may be filled in by the appropriate official of the Embassy of the requesting country.</p>
12. REQUESTING SECURITY AUTHORITY	<p><u>DO NOT FILL IN.</u></p> <p>Note for the requesting NSA/DSA:</p> <p>a. Mention name, address, telephone, facsimile numbers and e-mail (can be pre-printed).</p> <p>b. Sign and eventually stamp this item.</p>
13. REMARKS	<p>a. This item can be used for certain administrative requirements (e.g. proposed itinerary, request for hotel, and/or transportation).</p> <p>b. This space is also available for the receiving NSA/DSA for processing, e.g., "no security objections", etc.</p> <p>c. In case of an Emergency Visit the name, telephone, fax numbers and e-mail of the knowledgeable person (Doc. 7, section II, point 2a) should be stated.</p> <p>d. In case a special briefing is required, the type of briefing and the date that the briefing was given should be stated.</p>

REQUEST FOR VISIT		
<input type="checkbox"/> One-time <input type="checkbox"/> Recurring <input type="checkbox"/> Emergency <input type="checkbox"/> Amendment	<input type="checkbox"/> Unclassified/RESTRICTED information or access to areas without access to information classified CONFIDENTIAL or above <input type="checkbox"/> CONFIDENTIAL or above involved.	Annexes: <input type="checkbox"/> Yes <input type="checkbox"/> No
1. ADMINISTRATIVE DATA		
REQUESTOR:		DATE:
TO:		VISIT ID:
2. REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY		
NAME		
POSTAL ADDRESS		E-MAIL ADDRESS (when known)
TELEX/FAX NR.		TELEPHONE
3. GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED		
NAME		
ADDRESS		E-MAIL ADDRESS (when known)
TELEX/FAX NR.		TELEPHONE
POINT OF CONTACT		
4. DATES OF VISIT: // TO // (// TO //)		
5 TYPE OF VISIT: (SELECT ONE FROM EACH COLUMN)		
<input type="checkbox"/> GOVERNMENT INITIATIVE	<input type="checkbox"/> INITIATED BY REQUESTING AGENCY OR FACILITY	
<input type="checkbox"/> COMMERCIAL INITIATIVE	<input type="checkbox"/> BY INVITATION OF THE FACILITY TO BE VISITED	

6. SUBJECT TO BE DISCUSSED/JUSTIFICATION:		
7. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED		
8. IS THE VISIT PERTINENT TO:		SPECIFY
Specific equipment or weapon system	<input type="checkbox"/>	
Foreign military sales or export license	<input type="checkbox"/>	
A Program or Agreement	<input type="checkbox"/>	
A defense acquisition process	<input type="checkbox"/>	
Other	<input type="checkbox"/>	
9. PARTICULARS OF VISITORS		
NAME		
DATE OF BIRTH:		PLACE OF BIRTH:
SECURITY CLEARANCE:		ID/PP NR:
POSITION:		NATIONALITY:
COMPANY/AGENCY:		
NAME		
DATE OF BIRTH:		PLACE OF BIRTH:
SECURITY CLEARANCE:		ID/PP NR:
POSITION:		NATIONALITY:
COMPANY/AGENCY:		
10. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY		
NAME:		TELEPHONE/FAX NRS. E-MAIL-ADDRESS (when known):
SIGNATURE:		

11. CERTIFICATION OF SECURITY CLEARANCE (only if information or areas classified CONFIDENTIAL or above will be involved unless required by bilateral agreements)	
NAME:	
ADDRESS:	<div>STAMP</div>
SIGNATURE:	
12. REQUESTING NATIONAL SECURITY AUTHORITY:	
NAME:	
ADDRESS:	<div>STAMP</div>
SIGNATURE:	
13. REMARKS:	

GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED:

1. NAME :
ADDRESS :

TELEX/FAX NO	:	E-MAIL (when known)	:
POINT OF CONTACT	:	TELEPHONE NO	:

2. NAME :
ADDRESS :

TELEX/FAX NO	:	E-MAIL (when known)	:
POINT OF CONTACT	:	TELEPHONE NO	:

3. NAME :
ADDRESS :

TELEX/FAX NO	:	E-MAIL (when known)	:
POINT OF CONTACT	:	TELEPHONE NO	:

4. NAME :
ADDRESS :

TELEX/FAX NO	:	E-MAIL (when known)	:
POINT OF CONTACT	:	TELEPHONE NO	:

5. NAME :
ADDRESS :

TELEX/FAX NO	:	E-MAIL (when known)	:
POINT OF CONTACT	:	TELEPHONE NO	:

(Continue as Required)

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

APPENDIX C

Definitions

Unless otherwise noted, these terms and their definitions are for the purposes of this Manual.

Access. The ability and opportunity to gain knowledge of classified information.

Adverse Information. Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security.

Affiliate. Any entity effectively owned or controlled by another entity.

Approved Access Control Device. An access control device that meets the requirements of this manual as approved by the FSO.

Approved Built-in Combination Lock. A combination lock, equipped with a top-reading dial that conforms to UL Standard Number UL 768Group 1R.

Approved Combination Padlock. A three-position dial-type changeable combination padlock listed on the GSA Qualified Products List as meeting the requirements of Federal Specification FF-P-110.

Approved Electronic, Mechanical, or Electro-Mechanical Device. An electronic, mechanical, or electro-mechanical device that meets the requirements of this manual as approved by the FSO.

Approved Key-Operated Padlock. A padlock, which meets the requirements of MIL-SPEC-P-43607 (shrouded shackle), National Stock Number 5340-00-799-8248, or MIL-SPEC-P-43951 (regular shackle), National Stock Number 5340-00-799-8016.

Approved Security Container. A security file container, originally procured from a Federal Supply Schedule supplier that conforms to federal specifications and bears a "Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock. Such containers will be labeled "General Services Administration Approved Security Container" on the

face of the top drawer. Acceptable tests of these containers can be performed only by a testing facility specifically approved by GSA.

Approved Vault. A vault constructed in accordance with this Manual and approved by the CSA.

Approved Vault Door. A vault door and frame unit originally procured from the Federal Supply Schedule (FSC Group 71, Part III, Section E, FSC Class 7110), that meets Federal Specification AA-D-600.

Authorized Person. A person who has a need-to-know for classified information in the performance of official duties and who has been granted a PCL at the required level.

Classified Contract. Any contract requiring access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.) The requirements prescribed for a "classified contract" also are applicable to all phases of precontract activity, including solicitations (bids, quotations, and proposals), precontract negotiations, post-contract activity, or other GCA program or project which requires access to classified information by a contractor.

Classification Guide. A document issued by an authorized original classifier that identifies the elements of information regarding a specific subject that must be classified and prescribes the level and duration of classification and appropriate declassification instructions. (Classification guides are provided to contractors by the Contract Security Classification Specification.)

Classified Information. Official information that has been determined, pursuant to reference (b) or any predecessor order, to require protection against unauthorized disclosure in the interest of national security and which has been so designated. The term includes NSI, RD, and FRD.

Classified Information Procedures Act. A law that provides a mechanism for the courts to determine what classified information defense counsel may access.

Classified Visit. A visit during which a visitor will require, or is expected to require, access to classified information.

Classifier. Any person who makes a classification determination and applies a classification category to information or material. The determination may be an original classification action or it may be a derivative classification action. Contractors make derivative classification determinations based on classified source material, a security classification guide, or a Contract Security Classification Specification.

Cleared Commercial Carrier. A carrier authorized by law, regulatory body, or regulation to transport SECRET material and has been granted a SECRET facility clearance.

Cleared Employees. All contractor employees granted PCLs and all employees being processed for PCLs.

Closed Area. An area that meets the requirements of this manual for safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.

Cognizant Security Agency (CSA). Agencies of the Executive Branch that have been authorized by reference (a) to establish an industrial security program to safeguard classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. These agencies are: The Department of Defense, DOE, CIA, and NRC.

Cognizant Security Office (CSO). The organizational entity delegated by the Head of a CSA to administer industrial security on behalf of the CSA.

Colleges and Universities. Educational institutions that award academic degrees, and related research activities directly associated with a college or

university through organization or by articles of incorporation.

Communications Security (COMSEC). Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications.

Company. A generic and comprehensive term which may include sole proprietorships, individuals, partnerships, corporations, societies, associations, and organizations usually established and operating to carry out a commercial, industrial or other legitimate business, enterprise, or undertaking.

Compromise. An unauthorized disclosure of classified information.

CONFIDENTIAL. The classification level applied to information, the unauthorized disclosure of which reasonable could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Consignee. A person, firm, or government activity named as the receiver of a shipment; one to whom a shipment is consigned.

Consignor. A person, firm, or government activity by which articles are shipped. The consignor is usually the shipper.

Constant Surveillance Service. A transportation protective service provided by a commercial carrier qualified by SDDC to transport CONFIDENTIAL shipments. The service requires constant surveillance of the shipment at all times by a qualified carrier representative; however, an FCL is not required for the carrier. The carrier providing the service must maintain a signature and tally record for the shipment.

Contracting Officer. A government official who, in accordance with departmental or agency procedures, has the authority to enter into and administer contracts and make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his or her authority.

Contractor. Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.

Courier. A cleared employee, designated by the contractor, whose principal duty is to transmit classified material to its destination. The classified material remains in the personal possession of the courier except for authorized overnight storage.

Corporate Family. The corporation, its subsidiaries, divisions and branch offices.

Custodian. An individual who has possession of, or is otherwise charged with, the responsibility for safeguarding classified information.

Declassification. The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation.

Defense Articles. Those articles, services, and related technical data, including software, in tangible or intangible form, which are listed on the United States Munitions List (USML) of reference (v), as modified or amended. Defense articles exempt from the scope of section 126.17 of reference (v) are identified in Supplement No. 1 to Part 126 of reference (v).

Derivative Classification. The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification. Persons who apply derivative classification markings shall observe and respect original classification decisions and carry forward to any newly created documents any assigned authorized markings.

Document. Any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

Downgrade. A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect a lower degree of protection.

Embedded System. An IS that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem such as, ground support equipment, flight simulators, engine test stands, or fire control systems.

Escort. A cleared person, designated by the contractor, who accompanies a shipment of classified material to its destination. The classified material does not remain in the personal possession of the escort but the conveyance in which the material is transported remains under the constant observation and control of the escort.

Facility. A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For purposes of industrial security, the term does not include Government installations.

Facility (Security) Clearance (FCL). An administrative determination that, from a security viewpoint, a company is eligible for access to classified information of a certain category (and all lower categories).

Foreign Government Information (FGI). Information that is:

a. Provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

b. Produced by the U.S. pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof,

requiring that the information, the arrangement, or both are to be held in confidence.

Foreign Interest. Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States or its territories, and any person who is not a citizen or national of the United States.

Foreign National. Any person who is not a citizen or national of the United States.

ISL 2006-02 #22 (10-307, 10-509 and Appendix C). Definitions of “Foreign National” and “U.S. Person, (ISL96L-1 #3). The NISPOM definition of a “U.S. person” is different from the definition found in the State Department's International Traffic in Arms Regulation (ITAR). Only a U.S. citizen is eligible for a personnel security clearance. Therefore, the NISPOM definition of U.S. person is an individual who is a U.S. citizen. The ITAR uses a broader definition of U.S. person based on a person's right to be hired if he or she is qualified for a job (employment). Such employment does not establish the eligibility basis for a security clearance.

Procedures must be in place to ensure that non-U.S. citizens do not have access to U.S. classified and foreign government information. If the procedures to preclude such access are not deemed adequate by the IS Rep, a detailed Technology Control Plan will be required that includes special briefings, non-disclosure statements and more stringent access control measures.

Formerly Restricted Data (FRD). Information that has been removed from the RD category after DOE and the Department of Defense have jointly determined that the information: (1) relates primarily to the military utilization of nuclear weapons and (2) can be adequately safeguarded as NSI in the United States.

Freight Forwarder (Transportation Agent). Any agent or facility designated to receive, process, and transship U.S. material to foreign recipients. In the context of this manual, an agent or facility cleared specifically to perform these functions for the transfer of U.S. classified material to foreign recipients.

Government Contracting Activity (GCA). An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

Handcarrier. A cleared employee, designated by the contractor, who occasionally handcarries classified material to its destination in connection with a classified visit or meeting. The classified material remains in the personal possession of the handcarrier except for authorized overnight storage.

Home Office Facility (HOF). The headquarters company of a multiple facility organization.

Industrial Security. That portion of information security concerned with the protection of classified information in the custody of U.S. industry.

Information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Information Security. The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order.

Information System (IS). An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material.

Intelligence. The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information, that concerns one or more aspects of foreign nations or of areas of foreign operations, and that is immediately or potentially significant to military planning and operations.

Limited Access Authorization (LAA). Security access authorization to CONFIDENTIAL or SECRET information granted to non-U.S. citizens requiring such limited access in the course of their regular duties.

Material. Any product or substance on or in which information is embodied.

Multiple Facility Organization (MFO). A legal entity (single proprietorship, partnership, association, trust, or corporation) composed of two or more contractors.

National of the United States. A citizen of the United States or a person who, though not a citizen of the United States, owes permanent allegiance to the United States.

NOTE: 8 USC 1101(a)(22) (reference (x)) lists categories of persons born in and outside the United States or its possessions who may qualify as nationals of the United States. This subsection should be consulted when doubt exists as to whether or not a person can qualify as a national of the United States.

NATO Information. Information bearing NATO markings, indicating the information is the property of NATO, access to which is limited to representatives of NATO and its member nations unless NATO authority has been obtained to release outside of NATO.

Need-to-Know. A determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program.

Network. A system of two or more IS that can exchange data or information.

Original Classification. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required. (Only government officials who have been designated in writing may apply an original classification to information.)

Parent Corporation. A corporation that owns at least a majority of another corporation's voting securities.

Personnel (Security) Clearance (PCL). An administrative determination that an individual is

eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

Prime Contract. A contract let by a GCA to a contractor for a legitimate government purpose.

Prime Contractor. The contractor who receives a prime contract from a GCA.

Proscribed Information.

- a. Top Secret information;
- b. COMSEC information, except classified keys used for data transfer;
- c. RD as defined in reference (c);
- d. SAP information; or
- e. SCI.

Protective Security Service. A transportation protective service provided by a cleared commercial carrier qualified by the SDDC to transport SECRET shipments.

Reference Material. Documentary material over which the GCA, who lets the classified contract, does not have classification jurisdiction, and did not have classification jurisdiction at the time the material was originated. Most material made available to contractors by the DTIC and other secondary distribution agencies is reference material as thus defined.

Remote Terminal. A device for communication with an automated information system from a location that is not within the central computer facility.

Restricted Area. A controlled access area established to safeguard classified material, that because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but that is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.

Restricted Data (RD). All data concerning the design, manufacture, or use of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category pursuant to section 142 of reference (c).

SECRET. The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Security in Depth. A determination made by the CSA that a contractor's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility.

Security Violation. Failure to comply with the policy and procedures established by this Manual that reasonably could result in the loss or compromise of classified information.

Shipper. One who releases custody of material to a carrier for transportation to a consignee. (See "Consignor.")

Source Document. A classified document, other than a classification guide, from which information is extracted for inclusion in another document.

Special Access Program (SAP). Any program that is established to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. A Special Access Program can be created or continued only as authorized by a senior agency official delegated such authority pursuant to reference (b).

Standard Practice Procedures (SPP). A document(s) prepared by a contractor that implements the applicable requirements of this manual for the contractor's operations and involvement with classified information at the contractor's facility.

Subcontract. Any contract entered into by a contractor to furnish supplies or services for performance of a prime contract or a subcontract. For purposes of this Manual a subcontract is any contract, subcontract, purchase order, lease agreement, service agreement, request for quotation (RFQ), request for proposal (RFP), invitation for bid (IFB), or other agreement or procurement action between contractors that requires or will require access to classified information to fulfill the performance requirements of a prime contract.

Subcontractor. A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor, who enters into a contract with a prime contractor. For purposes of this Manual, each subcontractor shall be considered as a prime contractor in relation to its subcontractors.

Subsidiary Corporation. A corporation in which another corporation owns at least a majority of its voting securities.

System Software. Computer programs that control, monitor, or facilitate use of the IS; for example, operating systems, programming languages, communication, input-output control, sorts, security packages and other utility-type programs. Considered to also include off-the-shelf application packages obtained from manufacturers and commercial vendors, such as for word processing, spreadsheets, data base management, graphics, and computer-aided design.

Technical Data. Information governed by reference (v) and the Export Administration Regulation (EAR) (reference (y)). The export of technical data that is inherently military in character is controlled by reference (v). The export of technical data that has both military and civilian uses is controlled by reference (y).

TOP SECRET. The classification level applied to information, the unauthorized disclosure of which reasonable could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

Transmission. The sending of information from one place to another by radio, microwave, laser, or other

nonconnective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.

Transshipping Activity. A government activity to which a carrier transfers custody of freight for reshipment by another carrier to the consignee.

UK Community. Consists of the UK Government entities with facilities and non-governmental facilities identified on the DDTC website (<http://www.pmdtc.state.gov/>) at the time of export.

Unauthorized Person. A person not authorized to have access to specific classified information in accordance with the requirements of this Manual.

United States. The 50 states and the District of Columbia.

United States and its Territorial Areas. The 50 states, the District of Columbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, Wake Island, Johnston Atoll, Kingman Reef, Palmyra Atoll, Baker Island, Howland Island, Jarvis Island, Midway Islands, Navassa Island, and Northern Mariana Islands.

NOTE: *From 18 July 1947 until 1 October 1994, the United States administered the Trust Territory of the Pacific Islands; it entered into a political relationship with all four political units: the Northern Mariana Islands is a commonwealth in political union with the United States (effective 3 November 1986); the Republic of the Marshall Islands signed a Compact of Free Association with United States (effective 21 October 1986); the Federated States of Micronesia signed a Compact of Free Association with the United States (effective 3 November 1986); Palau*

concluded a Compact of Free Association with the United States (effective 1 October 1994).

U.S. Person. Any form of business enterprise or entity organized, chartered or incorporated under the laws of the United States or its territories and any person who is a citizen or national of the United States.

Upgrade. A determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a higher degree.

Voting Securities. Any securities that presently entitle the owner or holder thereof to vote for the election of directors of the issuer or, with respect to unincorporated entities, individuals exercising similar functions.

Working Hours. The period of time when:

a. There is present in the specific area where classified material is located, a work force on a regularly scheduled shift, as contrasted with employees working within an area on an overtime basis outside of the scheduled work shift; and

b. The number of employees in the scheduled work force is sufficient in number and so positioned to be able to detect and challenge the presence of unauthorized personnel. This would, therefore, exclude janitors, maintenance personnel, and other individuals whose duties require movement throughout the facility.

Working Papers. Documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

APPENDIX D

ISL Appendixes

ISL 2006-02 Appendix

Intrusion Detection System (IDS) Monitoring Over Data Networks

PURPOSE: This document identifies minimum acceptance criteria for the utilization of data networks for IDS alarm monitoring for the protection of classified material under the National Industrial Security Program Operating Manual (DoD 5220.22-M) (NISPOM). These data networks may include private data networks (intranets or virtual private networks/VPNs) or public data networks (*“the internet”*). This guidance establishes baseline security policies and requirements for sensitive, national security related applications and systems used for such alarm monitoring.

1. BACKGROUND:

- A. The NISPOM and the DoD Arms, Ammunitions & Explosives (AA&E) Manual (DoD 5100.76-M), specifies requirements regarding the use of IDS for the protection of classified material and certain risk categories of classified and unclassified AA&E. IDS utilized as supplemental protection for classified material as well as AA&E must comply with the Underwriters Laboratories standard for National Industrial Security Systems (UL 2050) for installation, testing, operations and maintenance. UL 2050 also identifies physical security measures for IDS when utilized for protection of DoD AA&E.
- B. UL 2050 provides the option of utilizing a *data network*¹ for alarm signal monitoring. While UL 2050 allows monitoring over data networks and specifies technical performance specifications,² it does not address security requirements, policies and procedures for IDS that utilize information systems (IS) for alarm signal monitoring over public or private communication lines. As NISPOM requirements apply only to classified information systems, additional guidance is needed to establish baseline security policies and requirements for sensitive, national security related applications and systems used for alarms.
- C. IDS' using data networks may range from the relatively simple (i.e. a contractor protected area connected directly through a static internet protocol (IP) network address to a Central Station Monitoring Service (CSMS), to the significantly complex [for example, hundreds of installations being remotely monitored over a corporate network at a Government Contractor Monitoring Station (GCMS).]

2. GUIDANCE:

- A. IDS' utilizing data network transmission shall be installed in conformance with appropriate UL 2050 requirements. All IDS equipment that is used to communicate with the data network shall be listed by UL for use with a data network, and the installation must result in the issuance of an appropriate UL 2050 certificate.

¹ UL 2050 describes data network transmission as “switching that sends packets of information from the alarm control/transmission panel in an alarmed area to a monitoring station by way of private data networks (intranets or virtual private networks/VPNs) or public data networks (*“the internet”*). A private data network is also known as a local area network (LAN) or a wide area network (WAN). “For the purpose of the standard, public data networks may also include WAN and/or Internet Protocol (IP) networks.

² Installation criteria, power, signal transmission, system operation, response personnel and procedures, timeframes, records, etc.

- B. Prior to installing an IDS [utilizing data networks for alarm system monitoring] for supplemental protection under the NISPOM, contractors will submit a request for approval to the CSA including the following information:
- (1) UL Alarm System Description for National Industrial Security Alarm System Certificate (Form No. CS-ASD-NISS);
 - (2) Proposed IDS hardware configuration and connectivity diagram (e.g. LAN/WAN schematic diagram) detailing the components (e.g. control panel, network interface cards, and method of data transfer (e.g. encryption implementation in hardware/firmware/software, etc.) between the protected area(s) and monitoring station locations. Hardware components and software will be identified by product name and release version.
- C. Depending on the type of installation (e.g. subscriber or monitoring station) and complexity of the IDS (as reflected in the hardware configuration and connectivity diagram,) the request must also address and certify compliance with the following requirements, as applicable:
- (1) **Government Contractor Monitoring Station (GCMS) or Central Station Monitoring Service (CSMS) IDS IS Server(s)/Host Computer:** The IDS IS Server(s) that receive and convert alarm signals to human readable form for appropriate assessment and response shall meet applicable UL requirements. The IS Server(s) running the IDS alarm signal processing software will be dedicated to the security system and staffed by monitoring personnel cleared to the Secret level. When monitoring personnel are not in attendance, the IDS IS [running IDS application software] will be secured within a locked room³ with UL certified Extent 3 IDS protection.⁴
 - (2) **Remote Terminals:** Networked terminals that allow privileged access to the IDS IS host computer (i.e. can program or modify system operating parameters or user accesses, etc.) shall be continuously staffed by authorized personnel or protected within a locked room³ with UL certified Extent 3 IDS protection. There shall be no capability for changing the mode of operation or status of the protected area(s) IDS from locations outside the authorized IDS staffed terminals or protected area(s).
 - (3) **Workstations:** Workstations are terminals that only provide for acknowledgement of alarm signals. Unattended workstations will be secured within a locked room³ with UL certified Extent 3 IDS protection.
 - (4) **User ID's and Passwords:** A unique user ID (UID) and password is required for each individual granted access to the IDS IS Server, remote terminal and workstation. Passwords shall be a minimum of eight characters; consist of alpha, numeric, and special characters; and shall be changed a minimum of every six months.
 - (5) **Personnel Security Clearance (PCL) Requirements:**
 - a. **Authorized Alarm Service Company (ASC) Representatives:** No clearance required. When working in IDS protected areas ASC representatives will be precluded from access to classified information and will be escorted/supervised by appropriately cleared personnel.

³ Rooms securing unattended IDS monitoring servers/host computers, remote terminals and/or workstations shall be comprised of walls, floors and ceilings that are fixed in place and constitute a solid physical boundary.

⁴ "Extent of Protection" is defined in paragraph 5.18 and Table 23.1, UL 2050.

- b. **System Administrator (SA):** The SA responsible for ensuring IDS IS server configuration, IDS communications signal processing software installation and updates, user account administration and maintenance will be cleared to the Secret level. For less complex IDS installations where the SA's duties are limited to the assignment of a network address/enabling of a network path for signal transmission between the protected area and monitoring station, a PCL will not be required. If the SA requires unescorted access to closed areas storing information above the Secret level, they will be cleared to the appropriate level consistent with the level of access and need-to-know.
 - c. **Information Technology (IT) Personnel:** There is no PCL required unless they have privileged access to the IDS server. Privileged access requires a Secret PCL. If IT personnel require full unescorted access to closed areas storing information above the Secret level, they will be cleared to the appropriate level consistent with the level of access and need to know.
 - d. **Users:** Personnel working in closed areas who arm/disarm the system will be cleared to the appropriate level of classified access
 - e. **Monitoring Personnel:** Secret PCL required.
- (6) **Intrusion Detection Software:** IDS IS server(s) and remote terminals running IDS application and signal processing software will utilize intrusion detection software to monitor and log access attempts and all changes to IDS applications. The SA and facility security supervisor will be notified of unauthorized system access attempts and/or modifications for investigation or other appropriate action. Records will be retained for a period of 12 months (from the date of entry.)
- (7) **IDS Signal Transmissions:** All IDS signal transmissions between the protected area (closed area) and the monitoring station shall be:
- a. Protected though firewalls or similar enhancements (e.g. routers, Virtual Private Networks/VPNs, etc.) that are configured to allow only protective signaling data transfers between IDS components and addresses; and
 - b. Encrypted using a National Institute of Standards (NIST) Federal Information Processing Standards (FIPS)⁵ approved algorithm with a key length of 128 bits⁶ (or greater); and,
 - c. Polled at a minimum of six minutes regardless of protected area alarm system status, i.e. open or closed.
- (8) **Service and Maintenance:** IDS IS testing, diagnostics, maintenance or programming will only be accomplished by the SA or ASC personnel, as appropriate. The ASC certifying alarm system installation and performing service, modifications or maintenance must be appropriately UL listed. While working in IDS protected areas, ASC personnel will be precluded from access to classified information and will be escorted by cleared and technically knowledgeable contractor employees. Unapproved use or substitution of non-UL listed IDS equipment or components can result in withdrawal of the UL certificate.

⁵ UL 2050 also requires that the cryptographic modules must be certified in writing by the equipment manufacturer as complying with the NIST FIPS 140-2. The NIST validation list is available at <http://csrc.nist.gov/cryptval/140-1/140val-all.htm>.

⁶ Both the *three-key* Triple Data Encryption Algorithm (TDEA) and the Advanced Encryption Standard (AES) algorithm (FIPS 197) are acceptable.

- (9) **Annual IDS Testing.** After initial testing and approval, the IDS shall be inspected and tested annually to provide assurances that the IDS is functioning properly in accordance with UL 2050 and the NISPOM.
- (10) **IDS Failure / Emergency Procedures:** In the case of IDS failure, closed areas storing Secret or Top Secret material, GSA approved security containers storing Top Secret material, or substandard security containers storing no higher than Secret classified material will be periodically inspected by appropriately cleared personnel in accordance with NISPOM standards for providing supplemental controls. Areas storing DoD AA&E material will be continuously staffed. Emergency procedures will remain in effect until the system is restored to operational status.
- D. The CSA will review the contractor's request for approval. The CSA representative (IS Rep or in the case of AA&E, the designated Contracting Officer Representative) may consult with the appropriate UL POC regarding compliance with UL standards. If the IDS request and Alarm System Description form reflects compliance with these requirements, the designated CSA representative will sign [on page 4 – Alarm Transmission for Data Networks] the Alarm System Description Form (CS-ASD-NISS) and maintain a copy of the form with the contractor documentation in the official facility file. The original will be provided to UL by the ASC or contractor, as appropriate. The CSA representative may then formally approve the proposed IDS as supplemental controls under the NISPOM.
- E. The ASC will submit the signed Alarm Systems Description for National Industrial Security Alarm System Certificate (CS-ASD-NISS) along with the [ASC completed] Alarm System Certificate Request (CS-R2) to UL for issuance of the CRZH certificate for the protected space. Form CS-R2 is a multi-copy form. A completed copy will remain with the alarm customer as proof of [UL] submittal until the completed certificate arrives.
- F. IDS currently approved in writing by a US Government cognizant security authority as meeting the requirements of DCID 6/9 for protection of SCI may be approved under the NISP provided the CSA approval was issued without waiving any requirements of the DCID 6/9 for Networked IDS. Alarm systems, procedures and related records approved for NISP use will be accessible for verification and review by DSS.
- G. If an IDS approved under these procedures are subsequently determined not to be in compliance with UL and NISPOM requirements, the approval will be rescinded and the contractor will be required to implement an alternative procedures for supplemental protection of classified material.

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

(This Page Intentionally Left Blank)

DoD 5220.22-M, Change 1, March 28, 2013
with ISLs 2006-01, -02; 2007-01; 2009-01, -02, -03;
2010-01, -02; 2011-01, -02, -03, -04; 2012-01, -02,
-03, -04; 2013-01, -02, -03, -04, -05, -06;
2014-01, -02, and -03
Compiled May 2, 2014

