Summary of Major NISPOM Changes

General

The term "contractor" used throughout the NISPOM means a cleared contractor; i.e., a contractor that has been granted a facility clearance (FCL).

The term "company" is used for those contractors that are not cleared or not yet granted an FCL.

The term "personnel" is used in place of "employees" to recognize that subcontractors fill many roles traditionally handled by company employees.

The use of a CSA-designated database; i.e., JPAS; for maintaining records of eligibility and access to classified information is incorporated throughout.

The Intelligence Reform and Terrorism Prevention Act of 2004 established the Office of the Director of National Intelligence (DNI) and changed the roles and responsibilities of the Director of the Central Intelligence Agency (CIA). The NISPOM has been changed to acknowledge that 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. The CIA is still designated as the CSA per Executive Order (EO) 12829 and the NISP Implementing Directive.

DoD publication policy requires certain formatting conventions, which have been incorporated into this version. Some minor wording modifications were required. A reference section has been added to this version, as well. This has resulted in a document that is less user-friendly, but meets the DoD publication requirements.

Note: This is a summary list of major changes. There are many other minor changes throughout the NISPOM that have not been listed.

CHAPTER 1 – General Provisions and Requirements

Section. 1. Introduction

1-103. Agency Agreements. The list of agencies with agreements with the Secretary of Defense is updated.

1-105. Composition of Manual. "COMSEC Supplement to the Industrial Security Manual for Safeguarding Classified Information," DoD 5220.22-S-1, August 1983, is cancelled.

Section 2. General Requirements

1-204. Cooperation with Federal Agencies and Officially Credentialed Representatives of Those Agencies. Officially credentialed representatives of government agencies; i.e., contractor investigators; are to be afforded the same level of cooperation as required for federal investigative agents.

Section 3. Reporting Requirements

1-301. Reports to be Submitted to the FBI. Actual, probable, or possible terrorism are added to the reporting requirement to the FBI.

1-302. Reports to be Submitted to the CSA.

Adverse information and changes in cleared employee status can be reported electronically via JPAS.

The requirement to identify representatives of a foreign interest is eliminated. Foreign affiliation is reviewed as part of the adjudication process.

The requirement to update the SF 328 every 5 years is eliminated. The form should be updated only when there are material changes to the information previously reported.

CHAPTER 2 – Security Clearances

General: Paragraphs pertaining to concurrent PCLs, conversions, terminations, and reinstatements are eliminated, as processes are now handled through JPAS.

Section 1. Facilities Clearances (FCLs)

2-108. Multiple Facility Organizations (MFOs). Adds the responsibility for the CSA to determine the necessity for branch offices of multiple facility organizations to be cleared.

Section 2. Personnel Security Clearances

2-200. General.

LOCs are eliminated. Notification of granting of eligibility for access to classified information; i.e., personnel security clearance (PCL); is accomplished by use of the JPAS.

The contractor is responsible for maintaining the records of its employees in JPAS.

Contractors within a corporate family may centrally manage the eligibility and access records (i.e., PCLs) of their employees in JPAS.

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

2-201. Investigative Requirements.

Requires the use of the electronic SF 86 (e-QIP).

Reinvestigation is added to the investigative requirements.

Financial disclosure is added to investigative requirements when the GCA advises that it is necessary. The employee should be afforded the opportunity to complete and submit the financial disclosure form in private.

2-202. Procedures for Completing the Electronic Version of the SF 86.

The FSO or a designee is required to review of the entire SF 86 completed by the employee for adequacy and completeness; however, the privacy of the individual must be maintained. The information on an employee's SF 86 must not to be used for any other purpose within the company.

The requirement for a contractor employee to witness fingerprinting is eliminated.

2-205. Pre-employment Clearance Action. The 180-day limitation for pre-employment clearance action is eliminated. Pre-employment clearance action is permitted provided that the commitment for employment indicates that employment will commence within 30 days of the granting of eligibility for a PCL.

2-209. Non-U.S. Citizens. Clarifies that LAA requests must have the concurrence of the GCA in all instances. The requirement to obtain the concurrence of the CSA in certain circumstances is eliminated.

2-211. Interim PCLs. Access to SCI or SAP information based on an interim PCL is a determination made by the government activity that is the granting authority.

2-212. Consultants. Consultants to GCAs must be processed for PCLs by the GCA in accordance with GCA procedures.

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

2-300. Policy. Clarifies that invalidation of the FCL should be taken only if the contractor is not negotiating an acceptable FOCI mitigation/negation measure in good faith.

2-301. Factors. Expands the factors to be considered to determine FOCI, FCL eligibility, and protective measures.

2-302. Procedures. Information provided on the SF 328 regarding FOCI should reflect the corporate family of the company vs. the individual company. It is not necessary to break down the information by subsidiary.

2-303. FOCI Action Plans.

Clarifies that preparation of the NID is the responsibility of the GCA and that the CSA will notify the GCA of the need for a NID.

Clarifies that DSS will not delay implementation of a FOCI action plan pending completion of a GCA's NID process as long as there is no indication that the NID would be denied.

CHAPTER 4 – Classification and Marking

General: Updated to reflect guidance in EO 12958, as amended, dated 23 March 2003.

Section 1. Classification

4-101. Original Classification.

Clarifies that originally classified information is owned by, produced by or for, or is under the control of the U.S. Government. Clarifies that only an original classification authority; i.e., a government official who has been designated in writing; may make a determination to originally classify information.

The definition of damage to national security, with regard to classification determination, now includes transnational terrorism.

4-102. Derivative Classification Responsibilities. Eliminates the requirement for manager/supervisor determination of classification, and manager/supervisor signature prior to transmission outside the facility.

4-107. Downgrading or Declassifying Classified Information. The contractor must seek the guidance of the GCA prior to taking any declassification action on material marked for automatic declassification.

Section 2. Marking Requirements

4-206. Portion Markings. Guidance on marking FGI and NATO information is in Chapter 10.

4-208. Markings for Derivatively Classified Documents.

The 10-year declassification exemptions are no longer valid. When the duration instruction on the source document is marked "X1 through X8" the "Declassify On" line

should indicate that that source material was marked with these instructions and the date of origin of the most recent source document as appropriate to the circumstances.

Reference to guidance on the permanent exemption from automatic declassification at 25 years (25X) is eliminated.

4-210. Marking Special Types of Material. The category of electronic messages now includes email.

4-216. Downgrading or Declassification Actions. The contractor must seek the guidance of the GCA prior to taking any declassification action on material marked for automatic declassification. Old classification markings shall be cancelled only if the GCA approves the declassification action.

CHAPTER 5 – Safeguarding Classified Information

Section 2. Control and Accountability

5-200. Policy. The requirement to maintain "External Receipt and Dispatch Records" is eliminated. There is still a requirement to include a receipt in a package.

5-202. Receiving Classified Material. Classified material must be received by an authorized person regardless of delivery method. This means that a cleared person has to get the Fed Ex or U.S. Post Office delivery directly from the Fed Ex or U.S. Postal Service employee.

5-203. Generation of Classified Material. Classified working papers retained for more than 30 days from creation for TS, or 180 days from creation for S and C material, must be marked in the same manner as a finished document.

Section 3. Storage and Storage Equipment

5-303. SECRET Storage. Clarifies that supplemental controls are required for storage of SECRET material in Closed Areas.

5-306. Closed Areas.

Clarifies that closed areas must be afforded supplemental protection during non-working hours.

Clarifies that closed areas must be secured by the approved locking device during working hours when the area is unattended. Supplemental controls are not necessary during working hours when the area is temporarily unattended.

Clarifies that procedures are necessary to ensure the structural integrity of closed areas above false ceilings and below raised floors.

The CSA may grant self-approval authority to the FSO for closed area approval.

5-311. Repair of Approved Containers. Procedures for container repair are removed. Repair standards are unchanged.

Section 4. Transmission

5-401. Preparation and Receipting. Eliminates the requirement to retain package receipts for 2 years.

5-404. CONFIDENTIAL Transmission Outside a Facility. Clarifies that a commercial carrier is not required to be cleared for CONFIDENTIAL transmissions.

5-410. Use of Couriers, Handcarriers, and Escorts. Eliminates the requirement to maintain receipt and dispatch records with regard to couriers, handcarriers, and escorts.

5-411. Use of Commercial Passenger Aircraft for Transmitting Classified Material. Eliminates reference to obsolete procedures regarding the use of commercial passenger aircraft.

5-412. Use of Escorts for Classified Shipments. The requirements for escorts apply only when an escort is determined to be necessary to ensure the protection of classified information during transport.

Section 7. Disposition and Retention

5-701. Retention of Classified Material. Clarifies that contractors are authorized to retain classified material received or generated under a contract for 2 years after contract completion unless the GCA advises to the contrary. If retention is not authorized, the remaining classified material should be destroyed unless the GCA requests its return.

5-703. Disposition of Classified Material Not Received Under a Specific Contract. Clarifies the retention period for material other than that received or generated under a specific contract.

5-705. Methods of Destruction. New crosscut shredders authorized for destruction of classified material must be from the NSA Evaluated Products List of High Security Crosscut Shredders.

5-706. Witness to Destruction. Witnesses to destruction are not limited to company employees, but may be subcontractors, as well.

Section 8. Construction Requirements

5-801. Construction Requirements for Closed Areas.

Closed Area construction is not limited to wood or metal. Walls and doors may be constructed of any material offering resistance to and detection of unauthorized entry.

A barrier is not required over miscellaneous openings if an approved IDS provides protection of the opening.

Adds an equivalent gauge commercial metal duct barrier to the options for covering miscellaneous openings in closed areas.

5-802. Construction Required for Vaults. Crossbars on rigid metal bars covering miscellaneous openings in vaults are only required on bars exceeding 18 inches in length.

Section 9. Intrusion Detection Systems

5-902. Central Monitoring Station. Clarifies that a sufficient number of SECRET cleared central station employees must be in attendance at the alarm monitoring station to monitor alarms.

5-903. Investigative Response to Alarms. A GCMS may be manned by cleared subcontractor security force personnel under a classified contract.

5-904. Installation.

Clarifies alarm installation standards as described in the U.L. 2050 installation guide.

Clarifies the conditions requiring CSA authorization on the Alarm System Description Form.

CHAPTER 6. - Visits and Meetings

Section 1. Visits

6-102. Need-to-know Determination. Eliminates the requirement to obtain GCA approval for non-contract related classified visits

6-104. Visit Authorization. Eliminates the requirement for a visit authorization letter (VAL) for classified visits within DoD when a CSA-designated database is available. Basically this means that within DoD, you do not need a VAL if you use JPAS.

6-105. Long-Term Visitors.

Clarifies that host contractor security procedures apply to government employees temporarily stationed at a contractor facility, but that contractors may not require government personnel to relinquish control of their work products to the contractor.

Clarifies that contractor employees at government installations follow the security requirements of the government host.

6-107. Visitor Record. Paragraph has been deleted which eliminates the requirement to maintain visitor records.

CHAPTER 7 – Subcontracting

Section 1. Prime Contractor Responsibilities

7-101. Responsibilities. Verification of subcontractor FCL and safeguarding capability may be accomplished by use of a CSA-designated database. (The database is currently identified as ISFD on the DSS website.)

CHAPTER 9 - Special Requirements

Section 1. Restricted Data and Formerly Restricted Data

Section provided by DOE, included for information purposes. Requirements for access to RD outlined in this section will be contractually imposed if applicable.

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

CNWDI access must be annotated in JPAS.

Section 3. Intelligence Information

Section provided by CIA and included for information purposes. Requirements for access to intelligence information will be contractually imposed, if applicable.

Section 4. Communications Security (COMSEC)

Section provided by NSA and contains general requirements for any contractor accessing COMSEC information. Any requirements beyond the NISPOM baseline must be contractually imposed.

CHAPTER 10 - International Security Requirements

General:

Many changes to eliminate information that was not relevant to the protection of classified information in industry.

"Government-to-government" terminology changed to "through government channels."

Eliminates the requirement for a separate briefing and written acknowledgement prior to contractor employees being granted access to FGI.

Standard Request for Visit Format (RFV) moved to Appendix B. Email addresses and fax numbers added to visit format. Lead time chart updated.

Section 2. Disclosure of U.S. Information to Foreign Interests

10-200. Authorization for Disclosure. Clarifies disclosure authorization formats.

10-201. Direct Commercial Arrangements. Clarifies disclosure of classified information pursuant to a direct commercial sale.

10-202. Contract Security Provisions. Reference to contract "provisions" versus "clauses."

Section 3. Foreign Government Information (FGI)

10-301. Contract Security Requirements. Clarifies that the foreign entity is responsible for providing appropriate security classification guidance.

10.303. Foreign Government RESTRICTED Information and "In Confidence" Information

Protection and marking requirements for Foreign Government RESTRICTED or "In Confidence" information are to be incorporated into the contract by the foreign government.

Foreign government RESTRICTED is to be protected as U.S. CONFIDENTIAL only if the contract requires that protection level.

10-306. Storage and Control. Eliminates the requirement for annual inventory of classified foreign government material.

10-308. Transfer. Clarifies that non-cleared express overnight carriers cannot be used for transfers of FGI.

Section 4. International Transfers

10-401. International Transfer of Classified Material. Eliminates the requirement for the DGR to be a U.S. Government employee.

10-402. Transfers of Freight. The transportation plan (TP) must address the need for escorts.

10-405. Handcarrying Classified Material. The CSA may authorize contractor employees to handcarry classified material outside of the United States in order to meet contractual requirements.

10-408. Transfers of Technical Data Pursuant to an ITAR Exemption. Clarifies signatory of written authorization for export of classified technical data.

Section 5. International Visits and Control of Foreign Nationals

10-507. Visits by Foreign Nationals to U.S. Contractor Facilities. A visit authorization for a foreign national to a U.S. contractor is valid throughout the corporate family.

Section 6: Contractor Operations Abroad

10-605. Report of Assignment. Eliminates the requirement to report overseas assignments.

Section 7. NATO Information Security Requirements

10-702. NATO RESTRICTED. Updates the guidance regarding NATO RESTRICTED, clarifying that no FCL is required for the company, PCLs are not required for personnel, and certification and accreditation are not required for IS.

10-706. NATO Briefings. The record of NATO briefings and debriefings is maintained in JPAS.

10-713. International Transmission. Eliminates reference to NATO sub-control points.

10-716. Disposition. Clarifies that destruction certificates are not required for NATO CONFIDENTIAL.

APPENDIX A - Cognizant Security Office Information

Refers to the DSS website.

APPENDIX B - International Visits Standard Request for Visit Format (RFV)

Contains the “Standard Request for Visit” format to be used for foreign visits.