DEFENSE SECURITY SERVICE

SELF-INSPECTIONS

October 2009

Table of Contents

I. SELF-INSPECTION CHECK-LIST

This Self-Inspection Check-List applies to individual cleared facilities. All sections of this form A-N must be addressed in order to ensure a thorough self-inspection. If the Self-Inspection reveals security violations or other reportable information, they must be reported to the appropriate DSS OGC.

A. Facility Security Clearance:

1. What changes have taken place during the past year that impacted the security program (i.e., changes in business structure, reporting chain, key management personnel, ownership, etc.)? NISPOM (1-302g(3))

2. Is your company required to submit an SF-328, Certificate Pertaining to Foreign Interests? If not, please describe how your facility's information is submitted for consolidated roll up reporting and identify what has been reported since the last inspection and who at the facility is responsible to review this information. NISPOM (2-302)

3. Has the FCL within the company been used for advertising or promotional purposes? If so, please explain. NISPOM (2-100c)

B. Access Authorizations:

Provide number of personnel clearances at the facility: TS _____ S _____ C _____

1. Who has access to JPAS at your facility? NISPOM (2-200)

2. Describe how JPAS accounts are/have been obtained by personnel at your facility. (NISPOM 2-200b; Procedures Governing Use of JPAS by Cleared Contractors, DSS April 2007)

3. How many individuals have JPAS Account Manager privileges at your facility? (NISPOM 2-200b; Procedures Governing Use of JPAS by Cleared Contractors, DSS April 2007)

4. Have all JPAS account holders successfully completed the Personally Identifiable Information (PII) course and signed the User's Certification? (NISPOM 3-102; DSS Special Alert 8/22/2008)

5. Do the JPAS users have the proper credentials (eligibility and minimum of a NACLC investigation)? (NISPOM 2-201b; ISL 2006-02 article #9)

6. How are the JPAS accounts monitored to ensure proper usage and identify misuse? (NISPOM 2-200 b; Procedures Governing Use of JPAS by Cleared Contractors, DSS April 2007)

7. Describe any incidents that involve the misuse of the JPAS account. (NISPOM 2-200b; Procedures Governing Use of JPAS by Cleared Contractors, DSS April 2007)

8. Has all the information in JPAS pertaining to cleared employees been validated? Does each record indicate appropriate "access" and "eligibility?" (NISPOM 2-200b)

9. Describe the process for having employees complete and submit their SF 86, including fingerprinting, verification of citizenship, and the review process. (NISPOM 2-202, NISPOM 2-207)

10. What adverse information reports have been submitted since the last inspection? Describe the criteria used by the organization when deciding to submit adverse information reports. (NISPOM 1-302a)

11. Have any cleared personnel been fired or dismissed since the last inspection? If so, please provide associated details including a copy of the associated adverse information report(s). (NISPOM 1-302a)

12. Describe the process that ensures the number of clearances is held to a minimum consistent with contractual requirements. (NISPOM 2-200d)

13. Are pre-employment offers for positions that require personnel security clearances (PCLs) made? If so, are the offers based on acceptance to begin employment within 30 days of granting eligibility for an interim or final PCL? (NISPOM 2-205)

C. Security Education:

1. What training has the Facility Security Officer (FSO) and security staff completed since the last inspection? Does the FSO have other responsibilities at the facility? If so, describe how the company ensures that the FSO has the time to devote to security matters. (NISPOM 3-102)

2. Describe the contents of security briefings provided to employees since the last inspection (initial, annual/refresher, and specialized briefings). How is the success of this training measured? (NISPOM 3-106, 3-107)

3. Which cleared employees who have contact with foreign nationals have been identified for specialized threat awareness training? (NISPOM 3-106, 3-107)

4. Do the FSO and other key security and management personnel have a thorough understanding of the foreign collection threat relevant to the facility and DoD equity residing therein? (NISPOM 3-106, 3-107)

5. Have representatives from any federal government CI, intelligence, or law enforcement agencies provided any threat awareness training at the facility since the last inspection?

If so, which agencies? Were the threat briefings provided by other agencies in relation to specific programs/technologies/contracts? (NISPOM 3-106, 3-107)

6. Have any suspicious incidents or issues involving cleared personnel to any federal government agencies been reported? If so, please explain. Was DSS also notified? If not reported to DSS, why? Have any other government agencies requested or implied that you not submit reports to DSS? (NISPOM 1-301, 1-302a, 1-302b)

7. Does the facility have a graduated scale of disciplinary action, table of disciplinary actions or other similar document? If so, was this scale followed in all cases of employees involved in security violations since the last inspection? Provide details. (NISPOM 1-304)

8. Has the (FSO) completed required training? If not, is training scheduled? Does the FSO and/or members of the staff attend local NCMS, ISAC, etc., meetings? (NISPOM 3-102)

9. Does the facility have any off-site locations? If so, what is the process to ensure personnel assigned off-site receive security education and training? (NISPOM 3-104)

10. Are employees aware of the Defense Hotline? If so, where is the information posted? (NISPOM 1-207)

D. Consultants:

1. Identify consultants used for classified services and the programs they support. A current 1099 and DD 254 t verifying classified work performed during the past year should be available during the inspection. (NISPOM 2-212)

2. Has the company and the consultants jointly executed a consultant certificate or consultant agreement setting forth respective security responsibilities? If so, please attach a copy. (NISPOM 2-212)

3. Has the criteria that establishes that the individual meets the definition of consultant versus subcontractor been validated? (NISPOM 2-212)

4. Does the consultant possess classified material at his/her place of business? If so, provide details. (NISPOM 2-212)

E. System Security Plan:

1. Has a System Security Plan (SSP) been compiled? If so, has the SSP been reviewed and updated (if necessary) since the last security review? (NISPOM 1-202)

F. Subcontracting:

1. Explain the process of releasing classified information to subcontractors. How is the need for classified access determined? How is classification guidance provided? During the past year, under which programs has classified material been released to subcontractors? (NISPOM 7-101)

2. Provide a listing of all classified subcontracts and include program names and contact information. (NISPOM 7-102)

3. Identify who at the facility has access to ISFD for facility verifications? Is an ISFD report on file for all subcontractors? (NISPOM 7-101)

4. Are all required actions completed prior to release or disclosure of classified information to subcontractors? (NISPOM 7-101)

5. Are contractor-prepared Contract Security Classification Specifications (DD 254) signed by a designated contractor official? (NISPOM 7-102)

6. Do requests for facility clearances or safeguarding include the required information? Has the facility sponsored another facility for an FCL? If so, review the request to ensure completeness? (NISPOM 7-101)

G. Visit Control:

1. What classified visits have taken place at the facility since the last inspection? How were visitors identified, their clearances verified, and need-to-know established? (NISPOM 6-101)

2. Describe where classified visits took place and how visitors were only afforded access to classified information consistent with the purpose of the visits. (NISPOM 6-101)

3. Describe visitor escort procedures and any related security incidents since the previous inspection. (NISPOM 6-101)

H. Classified Meetings:

1. Have any classified meetings taken place at the facility since the last inspection? If so, where were these meetings held and what procedures were followed? (NISPOM 6-201)

2. Did the government contracting activity sponsoring the meeting approve all security arrangements, announcements, attendees, and location? (NISPOM 6-201)

3. Describe procedures that ensure meeting attendance is limited to appropriately cleared persons with a verified need-to-know. (NISPOM 6-201)

I. Classification Guidance:

1. Provide a listing of all classified contracts either issued to the facility or being worked on by the facility, including program(s) name, contact information, and location of applicable security classification guides (SCGs). (NISPOM 4-103)

2. Are the SCGs adequate or do they contain unclear language? Explain and include actions taken to resolve any inconsistency with your customer(s). (NISPOM 4-103, 4-104)

3. Describe security incidents that have taken place since the last inspection as a result of classification guidance issues (security violations, marking issues, etc.). (NISPOM 4-105, 4-107)

4. Access Requirements: _____NATO _____CNWDI _____ COMSEC_____

5. Are employees designated to perform derivative classification actions sufficiently trained and do they have access to appropriate classification guidance? Identify designated personnel. (NISPOM 4-102)

6. Is all derivatively classified material appropriately marked? (NISPOM 4-102)

7. Upon completion of a classified contract describe the procedure for taking associated disposition action and/or requesting retention authority. (NISPOM 4-103)

J. Employee ID:

1. Describe the process for issuance and use of identification badges. If there have been issues, please explain. (NISPOM 5-313b)

2. Do personnel possess the required identification when employed as couriers, hand-carriers, or escorts? If there have been issues, please explain. (NISPOM 5-410b)

K. Public Release:

1. Who is responsible for submitting public release requests at your organization and what were the results of those requests (provide details)? (NISPOM 5-511)

2. Was approval of the Government Contracting Activity obtained, prior to public disclosure of information pertaining to a classified contract? (NISPOM 5-511)

L. COMSEC:

1. Identify type of COMSEC account (Traditional/SOCA) and account number: _____

2. Name of COMSEC Custodian and Alternate: _____

3. Describe briefing that is provided to all employees that require access to COMSEC information. (NISPOM 9-404)

M. Foreign Ownership, Control, or Influence (FOCI):

1. Is a signed original copy of the SF 328 accessible? Describe any material changes since the last submission to DSS. (NISPOM 2-302)

2. Who is responsible for reviewing the SF 328 and reporting the changes to DSS? How is this coordinated within the company? (NISPOM 2-302)

3. If operating under a FOCI Mitigation Instrument: (NISPOM 2-308)

    a. Attach a copy of the annual report presented to DSS.

    b. Describe the duties and involvement of the outside directors. How often are they present at the company?

    c. Provide an updated listing of affiliate companies. For home office facilities, provide a corporate structure diagram for all branch offices.

    d. Describe any violations/issues pertaining to the facility Technology Control Plan (TCP) or Electronic Communications Plan (ECP)?

    e. Have the ECP and TCP been updated to reflect the current organizational and operational requirements of the facility? Explain updates/changes.

    f. Describe any services provided by the foreign parent.

    g. Do any of your contracts involve prescribed information? If so, has a National Interest Determination been approved? Is any such access anticipated?

    h. Within a multiple facility organization, how has the FOCI Mitigation Instrument been implemented at the divisions?

    i. What training is provided to employees concerning the FOCI Mitigation Instrument?

    j. What efforts have been initiated to ensure compliance with the FOCI Mitigation Instrument? What is the process for verifying that these efforts are effective?

N. Classified Storage (If this facility does not store classified information, mark "NONE" here, and skip this section, and the next [?] sections):

1. Identify number of containers and types: GSA _____ Non GSA _____

2. Number of documents (including media): TS_____ S_____ C_____
   Number of pieces of hardware: TS _____ S_____ C_____

3. Provide the names of document control custodians and locksmith (or individual responsible for changing combinations to security containers). (NISPOM 5-308, 5-309)

4. Describe how need-to-know is established for access to security containers. (NISPOM 5-308)

5. Have any security containers been repaired or modified since the last inspection? If so, provide details. (NISPOM 5-311)

O. Markings:

1. Describe the process that employees follow when generating and marking classified material. How is success of this process measured from the last inspection? (NISPOM 4-200)

2. Is there any special caveat information such as (NATO, COMSEC, FRD/RD, CNWDI)? Under what contracts is this information held?? Have any subcontracts been issued that require access to special caveat information? (NISPOM 4-200)

3. What is the process to ensure that all classified material is properly marked? (NISPOM 4-200, 4-201)

4. Describe how employees who conduct derivative classification are trained? (NISPOM 4-208)

P. Transmission:

1. Explain the procedures for receiving classified material (i.e. hand-carry, US Mail, cleared courier). (NISPOM 5-202, 5-401)

2. What is the primary means for transmission at your facility? (NISPOM 5-402, 5-403, 5-404)

3. Is overnight delivery used for the transmission of classified information? If so, what carriers? Is there written approval from DSS for overnight transmission using commercial carriers? (NISPOM 5-403, 5-408)

4. Identify all individuals responsible for sending and receiving classified material at your facility. How are these individuals trained to perform this duty? (NISPOM 5-100, 5-202)

5. Describe any improper incoming/outgoing shipments of classified material. Were any items lost or compromised? (NISPOM 5-202, 5-401)

6. Describe the suspense system used to track transmitted documents until the signed receipt is returned. (NISPOM 5-401)

7. Identify who has hand-carried classified material during the past year. Describe the training for individuals with this responsibility. (NISPOM 5-410)

Q. Classified Material Controls:

1. Describe the information management system. How does it facilitate the retrieval and disposition of classified material? (NISPOM 5-200)

2. What specifically has been done since the last inspection to detect and deter the unauthorized removal or introduction of classified information? (NISPOM 5-103)

3. Describe the end-of-day check procedures. (NISPOM 5-102)

4. Have there been any losses, compromise or suspected compromise of classified material? Have there been any incidents which resulted in a determination of "no compromise?" Please provide details of all cases, including any that were not reported to DSS. (NISPOM 1-303)

5. Do emergency procedures exist for securing classified information? (NISPOM 5-104)

R. Controlled Areas:

1. Provide a list of all controlled areas and specify those activated since the last inspection.

2. Are there any areas that support multiple programs? Please list these and provide a copy of the Standard Operating Procedures (SOP) for the area(s) and customer approval letters. Have there been any issues in these areas since the last inspection? (NISPOM 5-306)

3. Describe supplemental controls in place at the facility. If Intrusion Detection System is used, does it meet UL 2050 or NISPOM standards? (NISPOM 5-303, 5-900, 5-901)

4. Has an alarm response to a closed area been required during the past year? Describe the incidents and identify if alarm response times were met. (NISPOM 5-900, 5-903)

S. Disposition:

1. Explain what has been done since the last inspection to review the facility's classified holdings. (NISPOM 5-700b)

2. Identify who is responsible for destroying classified material and if there have been any related issues. Identify all destruction equipment and methods. What types of information is being destroyed at the facility (i.e. media, documents, hardware)? (NISPOM 5-705, 5-706)

3. Have there been any requests for retention of classified material submitted since the last inspection? If so, please provide details. (NISPOM 5-701, 5-702)

T. Information Systems:

1. What is the facilities process for determining need to know for access to classified systems?

2. Who has performed trusted downloading over the past year and has your facility confirmed these were performed without error?

3. Have any virus contaminations, abnormal events, and unauthorized configuration changes taken place on classified systems? Have software applications been reloaded for these systems? If yes, explain what the situation was and what the investigation revealed.

4. Document any cases where the facility is unable to produce the past 12 months of records associated with an approved IS. Has the facility ruled out audit record tampering?

5. Identify the procedures for the removal of and introduction of material to classified systems. How is it ensured that systems are not contaminated with program material not approved for these systems?

6. Does the facility have multi-program information systems and letters from the Customers placing these programs on one system?

7. Does the company do any classified testing that employs the usage of making, coding, and disassociation schemes? If so please document what the facility is doing in this manner and provide and provide customer approval. If these are classified, acknowledge that these are performed and provide full particulars during the inspection.

8. Are there any Information Systems (IS) that have been accredited for classified processing by DSS? If so, provide the list of Unique Identifiers (UIDs). (NISPOM 8-202)

9. Are any IS operating under an Interim Authority to Operate (IATO)? If so, provide list including IATO expiration dates. (NISPOM 8-202)

10. Is there any IS that has been self-certified? If so, identify DSS approved Master Plan and Profile UID. (NISPOM 8-202)

11. Is there any IS that have not been accredited by DSS or self-certified that are being used to process classified information? If so, provide details. (NISPOM 8-202)

12. Was there any IS used for classified processing before it was accredited, self-certified, or after the accreditation expired? If so, provide details. (NISPOM 8-202)

13. Have any IS been used as mobile systems (sent to another contractor or government location)? If yes, please explain and identify DSS approved System Security Plan(s). (NISPOM 8-202)

U. Reproduction:

1. Identify all reproduction equipment. Has accreditation been requested when required? (NISPOM 8-202)

2. Who is responsible for reproduction of classified material and how is classified reproduction controlled? (NISPOM 5-600)

3. How did your facility approve the need for classified reproduction since the last inspection? (NISPOM 5-600)

V. International:

1. Identify any foreign classified contracts at the facility. (NISPOM 10-300, 10-301)

2. Provide the name of the individuals responsible for executing these contracts (i.e. Contracting Officer, Program Manager, Engineer). Describe the training that is provided to these individuals.

3. Is there a Designated Government Representative? If so, provide details. (NISPOM 10-401)

4. Identify any export controlled technologies, defense articles, or technical data at the facility. (NISPOM 10-200)

5. Provide a listing of all export authorizations (i.e., DSP 5, DSP 85, TAA, MLA) involving the transfer of classified material. (NISPOM 10-200)

6. Have there been any international hand-carriages of classified information to/from your facility since the last inspection? Identify employees designated as couriers, the programs involved, and any associated issues. (NISPOM 10-405)