

Suggested Contractor File Folder Headings

1. Facility Clearance
2. Personnel Clearances
3. Recurring Security Education
4. Self-Inspection
5. Security Correspondence
6. Standard Practice Procedures
7. Adverse Information Reports
8. Suspicious Contact Reports
9. Incoming Classified Visits
10. Visit Letters—Incoming Non-Contract Related
11. Visit Letters—Incoming Foreign
12. Visit Letters—Outgoing Foreign
13. DD Form 254—Active Contracts
14. DD Form 254—Completed Contracts/Retention
15. Security Container Combination Change Record
16. Information Management System (IMS)
17. Classified Material Receipts—Outgoing/Suspense
18. Physical Security Information
19. Destruction Certificates
20. IS Accreditation Letters
21. International
22. Security Violations
23. Industrial Security Letters (ISLs)

NOTE: The current DoD system of record is used to verify Personnel Access and Eligibility information, briefings, and terminations. As a result, contractors are not required to maintain obsolete paper records (e.g., Visit Letters, SF 312's, briefings, etc.).

File Folders #1 through #5 should be maintained by ALL cleared facilities.

FOLDER #1 – FACILITY CLEARANCE

1. Every cleared facility should have (and must also be uploaded into e-FCL):
 - a. DD Form 441 – DoD Security Agreement or DD Form 441-1 – Appendage to Security Agreement (if a division or operating location of an MFO)
 - b. KMP List (also include those KMP's who are excluded from access)
 - c. SF 328 – Certificate Pertaining to Foreign Interests

2. The following should be retained when applicable:
 - a. Resolution for Exclusion of Certain Officers and/or Directors
 - b. Letter temporarily Excluding Certain Officers and/or Directors from Access to Classified Material Pending a Formal Resolution by the Board
 - c. Resolution for Exemption of Parent Organization
 - d. Subsidiary Board Resolution Noting Parent's Exclusion and Resolution to Exclude Parent Organization
 - e. Certificates by Officers and/or Directors (Interlocking Officers and/or Directors)
 - f. Resolution of the Board of Directors of a Subsidiary Noting Non-Disclosure Certificates by Cleared KMP's serving in the same or similar capacities or positions with both the Subsidiary and Parent Organization (Interlocking Officers and/or Directors)
 - g. Certificate Covering Licenses, Patents, and other Foreign Affiliations (Resolution by the Board of Directors)
 - h. Letter indicating Assignment of CAGE Code

FOLDER #2 – PERSONNEL CLEARANCES

1. The current DoD System of Record is your official record of all cleared employees at your facility.
2. SF 86 and signed releases are required to be maintained until the time that the eligibility process is complete (these records should then be destroyed or returned to individual).
3. Consultant Agreement, if applicable.
4. Additional records you may elect to keep but are not required:
 - a. Copy of SF 312

- b. Special briefings/refresher briefings
- c. Violations
- d. Clearance justification, if applicable
- e. Evidence of citizenship
- f. Anything else you might find beneficial

FOLDER #3 – RECURRING SECURITY EDUCATION

1. Date and List of employees briefed.
2. Description of what was briefed to include copies of any materials provided: newsletters or articles used, etc.

FOLDER #4 – CONTRACTOR SELF-INSPECTION

1. Formal self-inspection report to include a description of the self-inspection, its findings, and resolution of issues found (retain through next CSA inspection).
2. Annual CSA certification that a self-inspection has been conducted, that senior management has been briefing on the results, and that management fully supports the security program. (via e-FCL.)

NISPOM Paragraph 1-207b states: Contractors shall review their security system on a continual basis and shall also conduct a formal self-inspection, including the self-inspection required by paragraph 8-101h of this Manual, at intervals consistent with risk management principles.

Additional Guidance for Self-Inspection Records:

- a. Suggest using the **SELF-INSPECTION HANDBOOK FOR NISP CONTRACTORS**. It is a helpful guide to use when performing your self-inspections and includes Insider Threat requirements. This handbook can be found at:
http://www.cdse.edu/documents/cdse/self_inspect_handbook_nisp.pdf

FOLDER #5 – SECURITY CORRESPONDENCE

1. File by latest date on top.
2. All material in this folder should be reviewed for disposition during each self-inspection.

File folders #6 through #27 should be maintained ONLY if they apply to the classified activities at your facility.

FOLDER #6 – STANDARD PRACTICE PROCEDURE (SPP)

1. Copy of your Standard Practice Procedure (SPP), if applicable.

NISPOM Paragraph 1-203 states: *The contractor shall implement all terms of the Manual applicable to 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 Cognizant Security Agency (CSA) determines them to be necessary to reasonably exclude the possibility of loss or compromise of classified information.*

NOTE: Discuss this requirement with your Industrial Security Representative and decide whether or not a SPP would be of benefit to your company's classified operation.

FOLDER #7 – ADVERSE INFORMATION REPORTS

1. In addition to completing the electronic "Incident Report" in the DoD System of Record, contractors may, if necessary, provide supplemental documentation (in hardcopy) relating to the incident report directly to the designated DSS entity.
2. Place in order by date of submission, last date on top, in alphabetical order by employee's name or in any other order you prefer.

FOLDER #8 – SUSPICIOUS CONTACT REPORTS (SCR)

1. File all submitted suspicious contact reports, last date on top.

FOLDER #9 – VISITS (INCOMING)

1. Although not required by the NISPOM, some contractors elect to maintain a record of incoming classified visitors. (Records are still required for foreign visitors - maintain for 1 year - and NATO visitors - maintain for 3 years.)
2. The current DoD System of Record is authorized to verify the visitor's personnel security access level (the visitor's access level and affiliation must be reflected), thereby eliminating the requirement for classified Visit Authorization Letters (VAL's).
3. If the visitor's personnel security access level cannot be verified in the DoD System of Record, a Visit Authorization Letter is required.

- a. Facilities must still have procedures in place to verify the identification of visitors and determining need-to-know prior to disclosing classified information.

FOLDER #10 – VISIT LETTERS (INCOMING - IF APPLICABLE)

1. Place in order by date of the letter, last date on top, in alphabetical order by the visitor's name, by company name, or in any other order you prefer.

FOLDER #11 – VISIT LETTERS (INCOMING FOREIGN)

1. Pertains to personnel visiting your facility from foreign countries.
2. Place in order by date of the letter, last date on top, in alphabetical order by visitor's name, or by any other order you prefer.
3. Maintain for one year.

FOLDER #12 – VISIT LETTERS (OUTGOING FOREIGN)

1. Pertains to employees making visits described in NISPOM Paragraph 10-502.
2. Place in order by date of the letter, last date on top, in alphabetical order by employee's name, or by any other order you prefer.

FOLDER #13 – DD FORM 254 (ACTIVE CONTRACTS)

1. DD Form 254(s) pertaining to active contracts and solicitations.
2. A listing of all current classified contracts should be placed in the front of each of these folders.
3. Copies of classification guides received for all classified contracts.
4. Public Disclosure Requests (see NISPOM paragraph 5-511a).

FOLDER #14 – DD FORM 254 (COMPLETED CONTRACTS)

1. DD Form 254 pertaining to inactive contracts, RFQ's, RFP's, and IFB's filed in numerical order by last four or five digits of contract, RFQ, RFP, or IFB. Separate by categories listed above.
2. Letter requesting authority to retain classified material, OR;
3. Final DD Form 254 or other correspondence authorizing retention of classified material beyond the automatic 2 year retention period.

NOTE: NISPOM authorizes an automatic two year retention period upon contract completion UNLESS you hear otherwise from your GCA or prime contractor. Retention must be requested for all SAP materials.

FOLDER #15 – SECURITY CONTAINER COMBINATION CHANGE RECORD

1. A record of the names of persons having knowledge of the combination. Standard Form 700, Security Container Information may be utilized. Not to be retained in same security container.
2. A record indicating the date of changes of security container combinations is optional. NISPOM paragraph 5-309 lists the events requiring the combination to be changed.

NOTE: Combinations for containers storing NATO classified information shall be changed annually (NISPOM Paragraph 10-712b).

FOLDER #16 – INFORMATION MANAGEMENT SYSTEM

1. Your Information Management System (IMS) shall be capable of facilitating the retrieval and disposition of your classified holdings in a reasonable time frame. This record could be an automated or a manual system.
2. Information captured in your IMS might include any combination of the following:
 - a. Date of material
 - b. Date material received
 - c. Where material was received from
 - d. Date material sent out/transmitted
 - e. Where material was sent
 - f. Classification level of the material
 - g. Unclassified description of material
 - h. Disposition of material & date thereof (required for TOP SECRET only)
 - i. Location of material/custodian
 - j. Contract number/retention authority for material
 - k. Control number (if applicable)
 - l. Number of copies (required for TOP SECRET only)
 - m. Any other information you find beneficial

3. For TOP SECRET, material must be numbered in a series (the copy number shall be placed on TOP SECRET documents and on all associated transaction documents) and the transmittal must be covered by a continuous receipt system both within and outside the facility.

FOLDER #17 – CLASSIFIED MATERIAL RECEIPTS OUTGOING/SUSPENSE

1. File in chronological order by the date the documents were sent out, earliest date on top.
2. Check weekly. Follow-up letter should be forwarded to addressee if signed receipt is not received in a reasonable length of time.
3. Remove and destroy when signed receipt is received.

FOLDER #18 – PHYSICAL SECURITY INFORMATION

1. Retain a copy of the DSS Form 147, Controlled Area Agreement, issued by the Cognizant Security Office.
2. Closed Area Self Approval Letter
3. UL Alarm Certificates
4. Shared Services Agreements
5. Letters Authorizing Security-In-Depth
6. MOAs or MOUs
7. Approval for Open Storage in Closed Areas
8. Any other physical security documentation that may apply to your security program.

FOLDER #19 – DESTRUCTION CERTIFICATES - REQUIRED FOR TS ONLY

1. File in order by date the material was destroyed, last date on top.
2. Include control number assigned by the facility on the Destruction Certificate.
3. Include the words “LAST ITEM” under the last document listed on the form.
4. Each page of the Destruction Certificate will be signed by the destroying and witnessing official.

5. Destruction Certificates may be numbered with the last digits of the year, followed by a dash and numerical sequence (e.g., 00-01, 00-02, 00-03, etc.).
6. TOP SECRET destruction records must be maintained by the contractor for a minimum of 2 years.
7. May also want to maintain a record of TS destruction with the classified contract it supports.

FOLDER #20 – INFORMATION SYSTEMS (IS) ACCREDITATION/AUTHORIZATION LETTERS

1. File all accreditation/authorization letters received from the Defense Security Service Field Office for the use of IS equipment for processing of classified material.
2. File in order by date of the authorization or by system number or identification.
3. Self-Accreditation Letters.

FOLDER #21 – INTERNATIONAL

1. Copies of all current export licenses involving classified materials (these would be received from the Department of State).
2. Technical Assistance Agreement (TAA).
3. Technology Control Plan (TCP).
4. Any other records pertaining to your company's international operation.

FOLDER #22 – SECURITY VIOLATIONS

1. Copies of all violation reports resulting in no compromise since the last government assessment.
2. Copies of all submitted violation reports resulting in loss, compromise, or suspected compromise.
3. Copies of any culpability reports submitted as a result of a violation resulting in loss, compromise, or suspected compromise.

FOLDER #23 – INDUSTRIAL SECURITY LETTERS

ISLs (2006 and beyond), as well as an ISL Quick Reference Tool, are posted and available on the DSS web-site at: http://www.dss.mil/isp/fac_clear/download_nispom.html

This Suggested Contractor File Folder Headings job aid is available in the FSO Toolkit, on the FSO page, under the Best Practices heading at: <http://www.cdse.edu/toolits/fsos/new-fso.html>