Request for Records Disposition Authority

(See Instructions on reverse)

To: **National Archives and Records Administration (NIR)**
Washington, DC 20408

1. From: (Agency or establishment)
Defense Security Service

2. Major Subdivision
Industrial Security

3. Minor Subdivision

4. Name of Person with whom to confer
Robert Crepeau

5. Telephone (include area code)
703-325-5344

Leave Blank (NARA Use Only)

Job Number
N1-446-09-5

Date Received
9/28/2009

Notification to Agency

In accordance with the provisions of 44 U.S.C. 3303a, the disposition request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10.

Date
2012 10

Archivist of the United States

6. **Agency Certification**

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal on the attached ___6___ page(s) are not now needed for the business of this agency or will not be needed after the retention periods specified; and that written concurrence from the General Accounting Office, under the provisions of Title 8 of the GAO Manual for Guidance of Federal Agencies:

[X] is not required [ ] is attached [ ] has been requested

Signature of Agency Representative	Title	Date (mm/dd/yyyy)
	Records Manager	08/22/2008

7. Item Number	8. Description of Item and Proposed Disposition	9. GRS or Superseded Job Citation	10. Action taken (NARA Use Only)
	See Attached.		

Industrial Security Facility Case Files

This schedule updates prior schedule NC1-446-81-2 item 2, "Industrial Security Facility Case Files"

DSS maintains the official records of contractor facilities involved in the National Industrial Security Program [NISP]. The availability, accuracy, and condition of these files affect the agency's ability to respond to information requests from Congress and other governmental activities. The field office is the repository for these files.

Electronic Files will be included and maintained with the same retention as paper files including in the Industrial Security Facilities Database (ISFD).

The Industrial Security Facility Database (ISFD) tracks facility clearance information including facility clearance requests, facility verification requests and notifications that are sent when facility information changes. The system also provides standard and customized reports. The major components of the system are described below:

- Facilities Management allows the user to search facilities, view their facilities, and generate standard and ad hoc reports. Provides the capability for Industrial Security personnel to input actions performed directly related to oversight of cleared contractors, and the time associated with those actions.
- Facility Clearance Request allows the user to search and submit clearance requests. A clearance request is submitted when a user agency, facility, or other entity requests a clearance for the facility and initiates the clearance process. Email notifications are sent to the requestors when the clearance is issued.
- Facility Verification Requests allows the user to search existing verification requests, submit verification requests, and view their verifications. A Facility Verification Request is submitted when a requestor (User agency or a facility) wishes to be notified when certain information about a facility changes.
- Notifications allow the user to view all their notifications for facilities they submitted verification requests for.
- User Management allows the user to update user information.
- The system also provides separate online user's manuals for the external and internal users.

Select data from the following documents are entered into ISFD from Industrial Security Case Files (manual files):
-Sponsorship Letter
-DD Form 254, Contract Security Classification Specification
-DD Form 441, Department of Defense Security Agreement
-DD Form 441-1, Appendage to the Department of Defense Security Agreement
-Standard Form 328, Certificate Pertaining to Foreign Agreements
-List of Key Management Personnel (KMP)
-SF 328, Certificate Pertaining to Foreign Interest

ISFD contains the following types of information:

- Facility Identifier Information
- Facility Programs
- Facility Business Information
- Key Management Personnel
- Facility Legal Structure
- Facility Actions
- User Agency Information
- Facility Clearance Requests
- Facility Clearance Notifications
- Facility Verification Requests
- Facility Verification Notifications

1. Hard copy printouts created:

Destroy when no longer needed for administrative, legal, audit, or other operational purposes.

2. Terminated or Inactive Facility Files Retention

a. Files both manual and electronic for terminated NISP facilities are destroyed two years from the date of the facility security clearance (FCL) termination.

b. Files with Foreign Ownership Control and Influence (FOCI) material will be retained for 15 years then destroyed in accordance with NC1-446-85-1, item 12, "FOCI Case Files" schedule.

3. Denied, Suspended, or Revoked Facility Files Retention

a. Files both manual and electronic for facilities that have had FCLs denied, suspended, or revoked will be destroyed 62 months after the last action.

b. Files with FOCI material will be retained for 15 years then destroyed in accordance with the FOCI Case File Schedule.

4. Active Files

Manual File Format.

Manual electronic files will be have the same structure of the paper based with electronic files established for each facility, excluded parent and Information Systems (IS) subdivided as the paper files.

A file folder (paper or electronic) is established for each cleared facility, excluded parent organization and IS.

The record copy of the electronic file folder created on the shared enterprise drive for Industrial Security, each office of record, using the DSS Office symbol for file name, will have folder and a sub folder will be created for each facility using the CAGE code and facility name for file name.

Electronic Files will be maintained with the same retention as paper or other manual files included in the Industrial Security Facilities Database (ISFD).

a. Six-Part Facility File

(1). Part 1 - contains documents regarding the FCL, as follows: A copy of the DISCO telephone facility survey and clearance justification; a printout of the "Facility Profile" form from the Industrial Security Facilities Database (ISFD); DD Form 441, "Department of Defense Security Agreement," or DD Form 441-1, "Appendage to the Department of Defense Security Agreement," as applicable; Standard Form 328, "Certificate Pertaining to Foreign Interests," (SF 328 was approved in April 1997 to replace DD Form 441s) and associated correspondence (e.g., Special Security Agreements, Voting Trusts); the list of Key Management Personnel (KMP), which includes name, position, date of birth, place of birth, social security number, and clearance status (refer to Enclosure 20, "KMP List"), and appropriate documentation (MFR's, establishment of executive management committees, board exclusion resolutions, etc.) to support a decision to exclude [other]key management official(s) who would not require a PCL in connection with the FCL; DSS Form Letter 381-R, "Letter of Notification of Facility Security Clearance. "Correspondence regarding the status of the FCL, including upgrade, termination, and invalidation; documentation on approved contractor offsite locations (i.e., facility locations considered to be an extension of the main facility where classified work is performed); documentation concerning cleared employees assigned to uncleared locations; list of contractor employees assigned overseas; Waivers and Exceptions.

1. Destroy when superseded.

2. FOCI information is retained for 15 years then destroyed in accordance with the FOCI Case File Schedule.

(2) Part 2 - contains documents pertaining to the IS Rep's visits to the facility, as follows:

A copy of the "Action-Security Review" form from the ISFD, which is one part of the two-part security assessment report. Correspondence concerning the security review, such as the security review notification letter, letter to the management outlining the results of the security review, and the contractor's

response to the results letter. Other significant correspondence (such as emails conveying guidance) between the contractor and DSS.

1. Destroy two years or two security review cycles, whichever is longer. Retain the information until no longer needed to document an adverse security trend within the facility, unresolved discrepancies, or any special circumstances (e.g., FOCI, International, IS) and should annotate the document. Destroy two years after adverse security trend, unresolved discrepancies or special circumstances have been corrected, or resolved.

2. FOCI information is retained for 15 years then destroyed in accordance with the FOCI Case File Schedule.

(3) Part 3 - contains documents regarding adverse or sensitive security issues, as follows:

Copies of security violations and administrative inquiries, including a copy of the violation report with the processing documentation (if the volume of these reports exceeds the capacity of Part 3, a note will be placed in Part 3 explaining that a separate violation folder has been created for this facility); termination or suspension of contractor employee PCL; reports of suspicious contact or other unclassified counterintelligence correspondence.

1. Destroy three years or two security review cycles, whichever is longer. Retain the information until no longer needed to document an adverse security trend within the facility, unresolved discrepancies, or any special circumstances (e.g., FOCI, International, IS) and should annotate the document. Destroy two years after adverse security trend, unresolved discrepancies or special circumstances have been corrected, or resolved.

2. FOCI information is retained for 15 years then destroyed in accordance with the FOCI Case File Schedule.

(4) Part 4 - contains documents regarding the contractor's involvement in international programs, as follows:

Government-to-government transmissions of classified information and copies of transportation plans; classification guidance for foreign classified contracts issued on U.S. Government contracts, similar to a DD Form 254, "Contract Security Classification Guidance"; Export Authorizations (e.g., DSP 85, Manufacturing License Agreements, Technical Assistance Agreements); Copies of violation reports involving foreign classified material; Technology Control Plans (TCPs). Program/Project Security Instructions.

(a). Export licenses must be retained until they are complete or have expired. Completed or expired export licenses must be returned to the State Department.

(b) Retain the information until no longer needed to document an adverse security trend within the facility, unresolved discrepancies, or any special circumstances (e.g., FOCI, International, IS) and should annotate the document. Destroy two years after adverse security trend, unresolved discrepancies or special circumstances have been corrected, or resolved.

(c) FOCI information used in administering Insulating Agreements (including Special Security Agreements, Security Control Agreements and resulting reports, reviews, correspondence, and background papers) will be retained for 15 years then destroyed in accordance with the FOCI Case File Schedule.

(5) Part 5 - contains documents of a semi-permanent nature, as follows:

Special security requirements. Closed area agreements, as recorded on "Record of controlled Area (DSS Form 147)" (refer to Enclosure 22); Documentation concerning Security-In-Depth (SID) and equivalency determinations - The IS Rep must document each decision to approve or disprove SID at the facility and any equivalency determinations. The documentation must include justification for the determination; Long term and special visitor agreements; Consultant agreements; Government-required briefings DSS Form 214A, "DSS COMSEC Report-Seed Key Only COMSEC Account (SOCA);" DSS Form 214B, "DSS COMSEC Report- Traditional Account;" and any COMSEC account correspondence; DSS approval letters for the use of destruction equipment and public destruction facilitates; Consolidated list of accredited ISs

Destroy when superseded.

(6) Part 6 - contains documents regarding classification guidance, as follows:

List of classified contracts; DD Forms 254, "Contract Security Classification Specification"; Classification guides, typically referenced in the DD Form 254.

Destroy documents when superseded.

b. Two-Part Excluded Parent

A two-part folder for each excluded parent organization and should destroy the information when superseded. Part 1 of the file folder will contain the survey information, clearance information on the cleared subsidiary, the "Facility Profile" form from ISFD, the SF 328 for the excluded parent, exclusion resolutions, and the KMP list

for the excluded parent. Part 2 of the file folder will contain the "Action-Security Review" from ISFD and miscellaneous correspondence.

(1) Destroy three years or two security review cycles, whichever is longer.

Retain the information until no longer needed to document an adverse security trend within the facility, unresolved discrepancies, or any special circumstances (e.g., FOCI, International, IS) and should annotate the document. Destroy two years after adverse security trend, unresolved discrepancies or special circumstances have been corrected, or resolved.

(2) FOCI information is retained for 15 years then destroyed in accordance with the FOCI Case File Schedule.

c. Two-Part Information Systems (IS) Folder

Maintain a separate two-part folder for each IS accredited by DSS. The file must be maintained for the duration of the IS accreditation. Track the number of accredited ISs by maintaining a consolidated list in Part 5 of the six-part facility file. Each two-part file will contain the following:

IS Security Plan system in electronic or hardcopy format. The current accreditation letter and current correspondence relating to the IS (e.g., interim accreditation letter, accreditation withdrawal letter, network security profile). A "baseline" IS Security Plan. Some contractors use a baseline or standard IS Security Plan to document their overall IS operations, with addenda to document-specific system information. It is only necessary to maintain one copy of the baseline SPP, the amendments to the baseline IS Security Plan (i.e., the system-specific information) for the accredited system, and the DSS accreditation letter. Memorandums of Understanding/Agreements with User Agencies.

(1) Retain for the duration of the IS accreditation, hold inactive for two years then Destroy.

(2) Destroy the information in the folder when superseded.