

GENERAL RECORDS SCHEDULE 18

Security and Protective Services Records

Security and protective services records include the various files created by agencies to control and protect classified information; to protect Government facilities from unauthorized entry, sabotage, or loss; to ensure the adequacy of protective measures at privately owned plants given security cognizance by the Government; to determine loyalty and fitness of individuals employed by, or seeking employment from the Government; and to develop and implement plans for the protection of life and property under emergency conditions. Included are selected files of offices having Government-wide or agencywide responsibility for security and protective services programs. Also included are files of security units, guard forces, and other organizational elements documenting the control of classified information, access to facilities, and like matters.

This schedule authorizes for disposal records documenting administrative actions relating to the above functions. Records documenting Government-wide or agencywide security and protective services planning and programming, reflecting basic overall policies and determinations are not authorized for disposal by this schedule. Variations among agencies in methods of implementing statutory requirements for security and protective services result in dissimilarities in program documentation. The application of standard techniques of filing and disposition to such records through the medium of a General Records Schedule is therefore impractical. Any records created prior to January 1, 1921, must be offered to the National Archives and Records Administration (NARA) before applying these disposition instructions.

A new item has been added to this schedule to authorize the destruction of electronic mail and word processing records maintained by agencies in addition to the copy in the recordkeeping system. This item covers electronic copies of electronic mail and word processing records created and used solely to produce the recordkeeping copy, and electronic copies of electronic mail and word processing records that are needed in addition to the recordkeeping copy for dissemination, revision, or updating.

CLASSIFIED INFORMATION ACCOUNTING AND CONTROL RECORDS

Records accumulating from measures taken by agencies to protect classified information from unauthorized disclosure in accordance with Executive orders and statutory or regulatory requirements.

1. Classified Documents Administrative Correspondence Files. [See note after this item.]

Correspondence files pertaining to the administration of security classification, control, and accounting for classified documents, not covered elsewhere in this schedule.

Destroy when 2 years old.

[NOTE: This item does not cover records documenting policies and

procedures accumulated in offices having agencywide responsibilities for security and protective services programs.]

2. Document Receipt Files.

Records documenting the receipt and issuance of classified documents.

Destroy when 2 years old.

3. Destruction Certificates Files.

Certificates relating to the destruction of classified documents.

Destroy when 2 years old.

4. Classified Document Inventory Files.

Forms, ledgers, or registers used to show identity, internal routing, and final disposition made of classified documents, but exclusive of classified document receipts and destruction certificates and documents relating to Top Secret material covered elsewhere in this schedule.

Destroy when 2 years old.

5. Top Secret Accounting and Control Files. [See note after item 5b.]

a. Registers maintained at control points to indicate accountability over Top Secret documents, reflecting the receipt, dispatch, or destruction of the documents.

Destroy 5 years after documents shown on forms are downgraded, transferred, or destroyed.

b. Forms accompanying documents to ensure continuing control, showing names of persons handling the documents, intra-office routing, and comparable data.

Destroy when related document is downgraded, transferred, or destroyed.

[NOTE: Master files and data bases created to supplement or replace the records covered by item 5 are not authorized for disposal under the GRS. Such files must be scheduled on a Standard Form (SF) 115.]

6. Access Request Files.

Requests and authorizations for individuals to have access to classified files.

Destroy 2 years after authorization expires.

7. Classified Document Container Security Files. [See note after item 7b.]

a. Forms or lists used to record safe and padlock combinations,

names of individuals knowing combinations, and comparable data used to control access into classified document containers.

Destroy when superseded by a new form or list or upon turn-in of containers.

b. Forms placed on safes, cabinets, or vaults containing security classified documents that record opening, closing, and routine checking of the security of the container, such as locking doors and windows, and activating alarms. Included are such forms as SF 701, Activity Security Checklist, and SF 702, Security Container Check Sheet.

Destroy 3 months following the last entry on the form (see note).

[NOTE: Forms involved in investigations will be retained until completion of the investigation.]

FACILITIES SECURITY AND PROTECTIVE SERVICES RECORDS

Records relating to measures taken for the protection of Government-owned facilities and privately operated facilities given security cognizance by the Government from unauthorized entry, sabotage, or loss.

8. Security and Protective Services Administrative Correspondence Files. [See note after this item.]

Correspondence files relating to administration and operation of the facilities security and protective services programs, not covered elsewhere in this schedule.

Destroy when 2 years old.

[NOTE: This item does not cover records documenting policies and procedures accumulated in offices having agencywide responsibilities for security and protective services programs.]

9. Survey and Inspection Files. (Government-owned facilities)

Reports of surveys and inspections of Government-owned facilities conducted to ensure adequacy of protective and preventive measures taken against hazards of fire, explosion, and accidents, and to safeguard information and facilities against sabotage and unauthorized entry.

Destroy when 3 years old or upon discontinuance of facility, whichever is sooner.

10. Survey and Inspection Files. (privately owned facilities)

Reports of surveys and inspections of privately owned facilities assigned security cognizance by Government agencies and related documents.

Destroy when 4 years old or when security cognizance is terminated, whichever is sooner.

11. Investigative Files.

Investigative files accumulating from investigations of fires, explosions, and accidents, consisting of retained copies of reports and related documents when the original reports are submitted for review and filing in other agencies or organizational elements, and reports and related papers concerning occurrences of such a minor nature that they are settled locally without referral to other organizational elements.

Destroy when 2 years old.

12. Property Pass Files.

Property pass files, authorizing removal of property or materials.

Destroy 3 months after expiration or revocation.

13. Guard Assignment Files.

Files relating to guard assignments and strength.

a. Ledger records.

Destroy 3 years after final entry.

b. Requests, analyses, reports, change notices, and other papers relating to post assignments and strength requirements.

Destroy when 2 years old.

14. Police Functions Files.

Files relating to exercise of police functions.

a. Ledger records of arrest, cars ticketed, and outside police contacts.

Destroy 3 years after final entry.

b. Reports, statements of witnesses, warning notices, and other documents relating to arrests, commitments, and traffic violations.

Destroy when 2 years old.

c. Reports on contact of outside police with building occupants.

Destroy when 1 year old.

15. Personal Property Accountability Files.

Files relating to accountability for personal property lost or stolen.

a. Ledger files.

Destroy 3 years after final entry.

b. Reports, loss statements, receipts, and other documents relating to lost and found articles.

Destroy when 1 year old.

16. Key Accountability Files.

Files relating to accountability for keys issued.

a. For areas under maximum security.

Destroy 3 years after turn-in of key.

b. For other areas.

Destroy 6 months after turn-in of key.

17. Visitor Control Files.

Registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers.

a. For areas under maximum security.

Destroy 5 years after final entry or 5 years after date of document, as appropriate.

b. For other areas.

Destroy 2 years after final entry or 2 years after date of document, as appropriate.

18. Facilities Checks Files.

Files relating to periodic guard force facility checks.

a. Data sheets, door slip summaries, check sheets, and guard reports on security violations (except copies in files of agency security offices covered by item 24 of this schedule).

Destroy when 1 year old.

b. Reports of routine after-hours security checks that either do not reflect security violations or for which the information contained therein is documented in the files defined in item 24 of this schedule.

Destroy when 1 month old.

19. Guard Service Control Files.

a. Control center key or code records, emergency call cards, and building record and employee identification cards.

Destroy when superseded or obsolete.

b. Round reports, service reports on interruptions and tests, and punch clock dial sheets.

Destroy when 1 year old.

c. Automatic machine patrol charts and registers of patrol and alarm services.

Destroy when 1 year old.

d. Arms distribution sheets, charge records, and receipts.

Destroy 3 months after return of arms.

20. Logs and Registers.

Guard logs and registers not covered elsewhere in this schedule.

a. Central guard office master logs.

Destroy 2 years after final entry.

b. Individual guard post logs of occurrences entered in master logs.

Destroy 1 year after final entry.

PERSONNEL SECURITY CLEARANCE RECORDS

Records accumulating from investigations of personnel conducted under Executive orders and statutory or regulatory requirements.

21. Security Clearance Administrative Subject Files.

Correspondence, reports, and other records relating to the administration and operation of the personnel security program, not covered elsewhere in this schedule.

Destroy when 2 years old.

22. Personnel Security Clearance Files.

Personnel security clearance case files created under Office of Personnel Management procedures and regulations and related indexes maintained by the personnel security office of the employing agency.

a. Case files documenting the processing of investigations on Federal employees or applicants for Federal employment, whether or not a security clearance is granted, and other persons, such as those performing work for a Federal agency under contract, who require an approval before having access to Government facilities or to sensitive data. These files include questionnaires, summaries of reports prepared by the investigating agency, and other records reflecting the processing of the investigation and the status of the clearance, exclusive of copies of investigative reports furnished by

the investigating agency.

Destroy upon notification of death or not later than 5 years after separation or transfer of employee or no later than 5 years after contract relationship expires, whichever is applicable.

b. Investigative reports and related documents furnished to agencies by investigative organizations for use in making security/suitability determinations.

Destroy in accordance with the investigating agency instructions.

c. Index to the Personnel Security Case Files.

Destroy with related case file.

23. Personnel Security Clearance Status Files.

Lists or rosters showing the current security clearance status of individuals.

Destroy when superseded or obsolete.

24. Security Violations Files.

Case files relating to investigations of alleged violations of Executive orders, laws, or agency regulations for the safeguarding of national security information.

a. Files relating to alleged violations of a sufficiently serious nature that they are referred to the Department of Justice or Department of Defense for prosecutive determination, exclusive of files held by the Department of Justice or Department of Defense offices responsible for making such determinations.

Destroy 5 years after close of case.

b. All other files, exclusive of documents placed in official personnel folders.

Destroy 2 years after completion of final action.

25. Classified Information Nondisclosure Agreements.

Copies of nondisclosure agreements, such as SF 312, Classified Information Nondisclosure Agreement, signed by civilian and military personnel with access to information that is classified under standards put forth by Executive orders governing security classification. These forms should be maintained separately from personnel security clearance files. Agreements for civilian employees working for elements of the intelligence community must be maintained separately from the official personnel folder. For all other persons, these forms may be filed in the individual's official military personnel folder (for uniformed military personnel) or on the right side of the official personnel folder (for civilian employees).

a. If maintained separately from the individual's official

personnel folder.

Destroy when 70 years old.

b. If maintained in the individual's official personnel folder.

Apply the disposition for the official personnel folder.

EMERGENCY PLANNING RECORDS

Records accumulating from the formulation and implementation of plans, such as evacuation plans, for protection of life and property during emergency conditions.

26. Emergency Planning Administrative Correspondence Files. [See note after this item.]

Correspondence files relating to administration and operation of the emergency planning program, not covered elsewhere in this schedule.

Destroy when 2 years old.

[NOTE: This item does not cover records documenting policies and procedures accumulated in offices having agencywide responsibilities for emergency programs.]

27. Emergency Planning Case Files. [See notes after this item.]

Case files accumulated by offices responsible for the preparation and issuance of plans and directives, consisting of a copy of each plan or directive issued, with related background documents, EXCLUDING one record copy of each plan or directive issued, if not included in the agency's permanent set of master directives files.

Destroy 3 years after issuance of a new plan or directive.

[NOTES: (1) If the emergency plan is not included in the agency's master set of directives files, a record set must be maintained and scheduled for eventual transfer to the National Archives of the United States by submission of an SF 115 to NARA. (2) Emergency planning reports of operations tests, consisting of consolidated or comprehensive reports reflecting agencywide results of tests conducted under emergency plans are also permanent and must be scheduled for transfer to the National Archives of the United States by submission of an SF 115.]

28. Emergency Operations Tests Files.

Files accumulating from tests conducted under agency emergency plans, such as instructions to members participating in test, staffing assignments, messages, tests of communications and facilities, and reports EXCLUDING consolidated and comprehensive reports.

Destroy when 3 years old.

29. National Defense Executive Reserve (NDER) Case Files.

Case files for NDER reservists or applicants, maintained by agencies

with major mobilization responsibilities in cases of national security emergencies, including qualifications statement, other personnel and administrative records, skills inventory, training data, and other records relating to administration of the NDER program.

a. Case files on reservists.

Destroy 5 years after termination from NDER program.

b. Case files on individuals whose applications were rejected or withdrawn.

Destroy when 5 years old.

30. Electronic Mail and Word Processing System Copies.

Electronic copies of records that are created on electronic mail and word processing systems and used solely to generate a recordkeeping copy of the records covered by the other items in this schedule. Also includes electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination.

a. Copies that have no further administrative value after the recordkeeping copy is made. Includes copies maintained by individuals in personal files, personal electronic mail directories, or other personal directories on hard disk or network drives, and copies on shared network drives that are used only to produce the recordkeeping copy.

Destroy/delete within 180 days after the recordkeeping copy has been produced.

b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy.

Destroy/delete when dissemination, revision, or updating is completed.