GENERAL RECORDS SCHEDULE 5.6: Security Management Records

Security Management involves the physical protection of an organization's personnel, assets, and facilities (including security clearance management). Activities include: security operations for protecting agency facilities, staff, and property; managing personnel security; and insider threat protection.

Conditions and Exclusions

The following conditions and exclusions apply to all disposition authorities in this schedule.

1. Agencies must offer any records covered by this schedule that were created prior to January 1, 1921, to the National Archives and Records Administration (NARA) before applying disposition instructions in this schedule, except records covered by items 120 and 130. Agencies must offer records covered by items 120 and 130 to the National Archives if they were created prior to January 1, 1939.
2. This schedule does not apply to records related to federal law enforcement activities and federal correctional activities (including records about their uniforms and equipment, body camera records, criminal surveillance records, records on accidents or incidents in incarceration or detention facilities, etc). Law enforcement and correctional functions differ from security functions and include border and transportation security and immigration and naturalization services. For additional description of these activities, see the FAQs for GRS 5.6. Agencies engaging in these activities must schedule such records on agency-specific schedules.
3. This schedule does not apply to records related to securing data and information systems. GRS 3.2, Information Systems Security Records, covers such records.
4. This schedule does not apply to records about protecting and accessing information. GRS 4.2, Information Access and Protection Records, covers such records.

Item	Records Description	Disposition Instruction	Disposition Authority
010	**Security management administrative records.** Records about routine facility security, protective services, and personnel security program administration not covered elsewhere in this schedule. Includes: ● administrative correspondence ● reports, including status reports on cleared individuals ● staffing level and work planning assessments, such as guard assignment records ● administrative subject files	**Temporary.** Destroy when 3 years old, but longer retention is authorized if required for business use.	DAA-GRS-2021-0001-0001

Item	Records Description		Disposition Instruction	Disposition Authority
020	**Key and card access accountability records.** Records accounting for keys and electronic access cards.	**Areas requiring highest level security awareness.** Includes areas designated by the Interagency Security Committee as Facility Security Level V.	**Temporary.** Destroy 3 years after return of key, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0002
021		**All other facility security areas.** Includes areas designated by the Interagency Security Committee as Facility Security Levels I through IV.	**Temporary.** Destroy 6 months after return of key, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0003
030	**Security uniform and equipment tracking records.** Records tracking uniforms and equipment issued to security management personnel, including: ● firearms (type, serial number, manufacturer, caliber, firearm registration date, storage location data, etc.) ● communication devices issued to security personnel, such as mobile radios and walkie-talkies ● body armor such as bullet-proof vests ● police baton and holder ● handcuffs and keys **Exclusion:** Does not apply to uniform and equipment tracking records for federal law enforcement and correctional officers. federal law enforcement includes border and transportation security and immigration and naturalization services.		**Temporary.** Destroy 3 months after return of equipment, but longer retention is authorized if required for business use.	DAA-GRS-2021-0001-0002
040	**Property pass records.** Records authorizing removal of government and privately owned property or materials off premises owned or leased by the federal government. Also includes hand receipts when used by staff to physically remove property.		**Temporary.** Destroy 3 months after expiration or revocation, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0005

Item	Records Description		Disposition Instruction	Disposition Authority
050	**Misuse or irregularities investigation records.** Records about irregularities in handling mail and improper use or misuse of telephone calling cards and government charge or purchase cards. Includes, but is not limited to, postal irregularities reports and semi-annual reports on government charge card violations. **Exclusions:** 1. Mail service records; covered under GRS 5.5, Mail, Printing, and Telecommunication Service Management Records, item 020.		**Temporary.** Destroy 3 years after final action. Longer retention is authorized for business use.	DAA-GRS-2023-0007-0001
060	**Unclaimed personal property records.** Records accounting for non-government, personally owned property lost, abandoned, unclaimed, or believed stolen on premises owned or leased by the federal government. Includes: ● lost-and-found logs and release forms ● loss statements ● receipts ● reports	**Records for property valued over $500.** **Legal Citation:** 41 CFR 102-41.130	**Temporary.** Destroy when 3 years old or 3 years after the date title to the property vests in the government, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0007
061		**Records for property valued at $500 or less.** **Legal citation:** 41 CFR 102-41.130	**Temporary.** Destroy 30 days after the property is found, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0008
Facility and physical security records.				

Item	Records Description		Disposition Instruction	Disposition Authority
070	**Interagency Security Committee member records.** Records are agency copies of committee records documenting the administration, operation, and decisions of the committee. Includes: ● agendas ● meeting minutes ● best practice and standards documents ● funding documents for security countermeasures **Exclusion:** Records documenting the committee's establishment, organization, policy, membership, meetings, findings, recommendations, and accomplishments maintained by the Department of Homeland Security (DHS). DHS covers these records under an agency-specific schedule.		**Temporary.** Destroy when 10 years old, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0009
080	**Facility security assessment records.** Surveys and inspections of security and safety measures at government or privately owned facilities assigned a security awareness status by government agencies. Includes: ● facility notes ● inspector notes and reports ● vulnerability assessments	**Areas requiring highest level security awareness.** Includes areas designated by the Interagency Security Committee as Facility Security Level V.	**Temporary.** Destroy 5 years after updating the security assessment or terminating the security awareness status, whichever is sooner, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0010
081		**All other facility security areas.** Includes areas designated by the Interagency Security Committee as Facility Security Levels I through IV.	**Temporary.** Destroy 3 years after updating the security assessment or terminating the security awareness status, whichever is sooner, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0011

Item	Records Description	Disposition Instruction	Disposition Authority
090	**Facility security management operations records.** Records about detecting potential security risks, threats, or prohibited items carried onto federal property or impacting assets, including records documenting access control, screening, patrol and response, and control center operations. Includes: ● control center key or code records ● registers of patrol and alarm services ● service reports on interruptions and tests ● emergency alarm contact call lists ● temporary identification cards ● correspondence or lists of facility occupants authorized to enter with a prohibited or controlled item on an identified date ● round and perimeter check reports, including facility patrol tour data ● surveillance records that do not document accidents or incidents ○ recordings of protective mobile radio transmissions ○ video surveillance recordings ○ closed circuit television (CCTV) records ● door slip summaries **Exclusions:** The following records are excluded and must be scheduled on agency-specific schedules: 1. Records related to federal law enforcement and federal correctional activities, such as body camera recordings and criminal surveillance records. Federal law enforcement includes border and transportation security and immigration and naturalization services. 2. Records related to accident or incident investigations (see note 1 below). Surveillance recordings that include accidents or incidents may be destroyed using this disposition authority provided a copy is retained in the accident or incident investigation records. **Notes:** 1. Item 100 covers records of accidents and incidents. 2. Items 110 and 111 cover records of visitor processing.	**Temporary.** Destroy when 30 days old, but longer retention is authorized if required for business use.	DAA-GRS-2021-0001-0003

Item	Records Description		Disposition Instruction	Disposition Authority
100	**Accident and incident records.** Records documenting accidents and incidents occurring on, in, or at government-owned or -leased facilities, vehicles (land, water, and air), and property used by federal agencies. **Exclusions:** 1. Records of the Federal Aviation Administration (FAA) and the National Transportation Safety Board (NTSB) relating to aircraft used by federal agencies, including leased aircraft used by federal agencies. The FAA and NTSB cover these records under agency-specific schedules. 2. Records related to federal law enforcement and federal correctional activities. Federal law enforcement includes border and transportation security and immigration and naturalization services. Agencies that create these records must schedule them on agency-specific schedules. 3. Records of accidents or incidents in federal facilities involved in incarcerating or detaining individuals. Agencies that create these records must schedule them on agency-specific schedules. 4. Workers' compensation (personnel injury compensation) records. GRS 2.4, Employee Compensation and Benefits Records, items 100 and 101, covers these records. 5. Records that vehicle management offices maintain about vehicle and vessel accidents—land, water, and air. GRS 5.4, Facility, Equipment, Vehicle, Property, and Supply Records, item 140, covers these records.		**Temporary.** Destroy 3 years after final action. Longer retention is authorized for business use.	DAA-GRS-2023-0007-0002
110	**Visitor processing records.** Registers or logs recording names of outside contractors, service personnel, foreign national and other visitors, employees admitted to areas, and reports on vehicles and passengers. **Note:** GRS 4.2, Information Access and Protection Records, item 030, covers requests and authorizations for individuals to have access to classified files.	**Areas requiring highest level security awareness.** Includes areas designated by the Interagency Security Committee as Facility Security Level V.	**Temporary.** Destroy when 5 years old, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0014
111		**All other facility security areas.** Includes areas designated by the Interagency Security Committee as Facility Security Levels I through IV.	**Temporary.** Destroy when 2 years old, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0015

Item	Records Description		Disposition Instruction	Disposition Authority
120	**Personal identification credentials and cards.** Records about credential badges (such as smart cards) that are (1) based on the HSPD-12 standards for identification cards issued to federal employees, contractors, and affiliates, and (2) used to verify the identity of individuals seeking physical access to federally controlled government facilities, and logical access to government information systems. Also referred to as Common Access Cards (CAC) cards, Personal Identity Verification (PIV) cards, and Homeland Security Presidential Directive 12 (HSPD-12) credentials. **Exclusion:** Records of certain classes of government employee identification cards, such as those covered under special-risk security provisions or 44 U.S.C. Section 3542. Agencies must schedule these records on agency-specific schedules.	**Application and activation records.** Applications and supporting documentation, such as chain-of-trust records, for identification credentials. Includes: ● application for identification card ● a log of activities that documents who took the action, what action was taken, when and where the action took place, and what data was collected ● lost or stolen credential documentation or police report **Note 1:** Agencies must offer any records created prior to January 1, 1939, to the National Archives and Records Administration (NARA) before applying this disposition authority. **Note 2:** GRS 3.2, Information Systems Security Records, covers applications for access to information systems.	**Temporary.** Destroy 6 years after the end of an employee or contractor's tenure, but longer retention is authorized if required for business use.	DAA-GRS-2021-0001-0005
121		**Cards.**	**Temporary.** Destroy after expiration, confiscation, or return.	DAA-GRS-2017-0006-0017

Item	Records Description	Disposition Instruction	Disposition Authority
130	**Temporary and local facility identification and card access records.** Temporary employee, contractor, and occasional visitor facility and network identification access card and identity management system records. Identification verification credentials issued by facility or building managers to provide local verification credentials and cards issued by facility or building managers to provide local identification and access. Includes: ● temporary identification cards issued to temporary employees, contractors, and occasional visitors who do not meet the FIPS 201 Standard requirements for PIV issuance ● supplemental cards issued to access elevators ● personnel identification records stored in an identity management system for temporary card issuance ● parking permits **Note:** Agencies must offer any records created prior to January 1, 1939, to the National Archives and Records Administration (NARA) before applying this disposition authority.	**Temporary.** Destroy upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner, but longer retention is authorized if required for business use.	DAA-GRS-2021-0001-0006
140	**Sensitive Compartmented Information Facility (SCIF) accreditation records.** Physical security plans for SCIF construction, expansion, or modification. Includes: ● initial Fixed Facility Checklist ● pre-accreditation inspection report ● Construction Security Plan (CSP) ● TEMPEST Checklist	**Temporary.** Destroy when SCIF receives final accreditation, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0019

Item	Records Description		Disposition Instruction	Disposition Authority
150	**Sensitive Compartmented Information Facility (SCIF) inspection records**. Inspection records required by Intelligence Community Directive (ICD) 705. Includes: ● Fixed Facility Checklists ● accreditation authorization documents ● inspection reports, including Technical Surveillance Counter Measures (TCSM) reports, for the entire period of SCIF accreditation ● operating procedures ● Special Security Officer/Contractor Special Security Officer (SSO/CSSO) appointment letters ● memoranda of agreements (MOAs) ● Emergency Action Plans ● copies of any waivers granted by the Cognizant Security Authority (CSA) ● co-utilization approvals		**Temporary.** Destroy when 5 years old or after SCIF has been de-accredited for at least one year, whichever occurs sooner, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0020
160	**Canine (K-9) service records.** Records documenting acquisition, training, activities, care, retirement or death of canine partners.		**Temporary.** Destroy 3 years after the end of the canine's service. Longer retention is authorized for business use.	DAA-GRS-2023-0007-0003
Personnel security records.				
170	**Personnel security investigative reports.** Investigative reports and related documents agencies create or use to support initial favorable eligibility determinations, fitness determinations, and periodic	**Personnel suitability and eligibility investigative reports.**	**Temporary.** Destroy in accordance with the investigating agency instruction.	DAA-GRS-2017-0006-0022

Item	Records Description		Disposition Instruction	Disposition Authority
171	reinvestigations, or to implement a continuous evaluation program.	**Reports and records created by agencies conducting investigations under delegated investigative authority.**	**Temporary.** Destroy in accordance with delegated authority agreement or memorandum of understanding.	DAA-GRS-2017-0006-0023
180	**Personnel security and access clearance records.** Records about security clearances, and other clearances for access to government facilities or to controlled unclassified information, created to support initial favorable eligibility determinations, periodic reinvestigations, or to implement a continuous evaluation program. Includes: ● questionnaires ● summaries of reports prepared by the investigating agency ● documentation of agency adjudication process and final determination **Note:** GRS 3.2, Information Systems Security Records, items 030 and 031, covers Information system access records.	**Records of people not issued clearances.** Includes case files of applicants not hired. **Exclusion:** Copies of investigative reports covered in items 170 and 171.	**Temporary.** Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use.	DAA-GRS-2021-0001-0007
181		**Records of people issued clearances.** **Exclusion:** Copies of investigative reports covered in items 170 and 171.	**Temporary.** Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use.	DAA-GRS-2021-0001-0008
190	**Index to the personnel security case files.** Lists or reports showing the current security clearance status of individuals.		**Temporary.** Destroy when superseded or obsolete.	DAA-GRS-2017-0006-0026

Item	Records Description	Disposition Instruction	Disposition Authority
200	**Information security violations records.** Case files about investigating alleged violations of executive orders, laws, or agency regulations on safeguarding national security information. Includes allegations referred to the Department of Justice or Department of Defense. Includes final reports and products. **Exclusion 1:** Documents placed in Official Personnel Folders. GRS 2.2, Employee Management Records covers these records. **Exclusion 2:** Records of any subsequent investigations are covered under agency-specific schedules, such as Office of the Inspector General schedules.	**Temporary.** Destroy 5 years after close of case or final action, whichever occurs sooner, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0027
Insider threat records.			
210	**Insider threat administrative and operations records.** Records about insider threat program and program activities. Includes: ● correspondence related to data gathering ● briefing materials and presentations ● status reports ● procedures, operational manuals, and related development records ● implementation guidance ● periodic inventory of all information, files, and systems owned ● plans or directives and supporting documentation, such as: ○ independent and self-assessments ○ corrective action plans ○ evaluative reports **Note**: GRS 2.6, Employee Training Records, covers records on mandatory employee training about insider threats.	**Temporary.** Destroy when 7 years old, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0028

Item	Records Description	Disposition Instruction	Disposition Authority
220	**Insider threat inquiry records.** Records about insider threat program inquiries initiated or triggered due to derogatory information or occurrence of an anomalous incident. Includes initiated and final reports, referrals, and associated data sets. **Exclusion:** Records of any subsequent investigations are covered under agency-specific schedules, such as Office of the Inspector General schedules.	**Temporary.** Destroy 25 years after close of inquiry, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0029

230	**Insider threat information.** Data collected and maintained by insider threat programs undertaking analytic and risk-based data collection activities to implement insider threat directives and standards. Includes, but is not limited to: ● Counterintelligence and security information ○ personnel security files ○ polygraph examination reports ○ facility access records, including visitor records ○ security violation files ○ travel records ○ foreign contact reports ○ financial disclosure filings ○ referral records ○ intelligence records ● Information assurance information ○ personnel usernames and aliases ○ levels of network access ○ levels of physical access ○ enterprise audit data which is user attributable ○ unauthorized use of removable media ○ print logs ● Human resources information ○ personnel files ○ payroll and voucher files ○ outside work and activities requests ○ disciplinary files ○ personal contact records ○ medical records/data ● Investigatory and law enforcement information ○ statements of complainants, informants, suspects, and witnesses ○ agency, bureau, or department data ● Public information ○ court records ○ private industry data ○ personal biographical and identification data, including U.S. Government name check data ○ generic open source and social media data	**Temporary.** Destroy when 25 years old, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0030

Item	Records Description	Disposition Instruction	Disposition Authority
	Exclusion: Case files of any subsequent investigations are covered under agency-specific schedules, such as Office of the Inspector General schedules.		
240	**Insider threat user activity monitoring (UAM) data.** User attributable data collected to monitor user activities on a network to enable insider threat programs and activities to: ● identify and evaluate anomalous activity involving National Security Systems (NSS) ● identify and assess misuse (witting or unwitting), or exploitation of NSS by insiders ● support authorized inquiries and investigations **Exclusion:** Records of any subsequent investigations are covered under agency-specific schedules, such as Office of the Inspector General schedules. **Legal authority:** CNSSD No. 504, 4 February 2014	**Temporary.** Destroy no sooner than 5 years after inquiry has been opened, but longer retention is authorized if required for business use.	DAA-GRS-2017-0006-0031