

# DAA-GRS-2016-00xx

## Security Records (GRS 5.6)

This file contains three documents. The Draft Schedule is the proposed text of the new GRS in publication format. The Draft Appraisal Memorandum provides additional background explanation and includes the appraiser's justification for the retention decisions proposed in the schedule. The Crosswalk provides additional help in schedule implementation.

This schedule has not yet been entered into the Electronic Records Archives, pending finalization through agency and stakeholder review.

<i>Document</i>	<i>Page in this PDF</i>
Draft Schedule .....	2
Draft Appraisal Memorandum .....	16
Crosswalk to old GRS .....	31

**-DRAFT of 4-15-2016-**  
**GENERAL RECORDS SCHEDULE 5.6: Security Records**

This schedule covers records related to managing the protection of an organization’s personnel, assets, and facilities. Activities include: security operations for protecting agency facilities, staff and property, managing personnel security, and insider threat protection.

Related records are covered elsewhere in the GRS. Records related to securing data and information systems are listed in GRS 3.2, Information Systems Security Records. Records related to protection of and access to information are covered in GRS 4.2, Information Access and Protection Records.

Item	Records Description		Disposition Instruction	Disposition Authority
010	<p><b>Security administrative records.</b>  Records relating to routine office program support, administration, and operation of facility security, protective services, and personnel security. Includes:</p> <ul style="list-style-type: none"> <li>• status reports on cleared individuals and other reports</li> <li>• staffing level and work planning assessments, such as guard assignment records</li> <li>• standard operating procedures manuals</li> </ul> <p><b>Supersedes:</b>  GRS 18, item 8 (GRS 18, 1960, item 9) <i>2 years</i>  GRS 18, item 13a (GRS 18, 1960, item 14a) <i>3 years</i>  GRS 18, item 13b (GRS 18, 1960, item 14b) <i>2 years</i>  GRS 18, item 21 (NC1-GRS-80-1, item 22) <i>2 years</i></p>		<p><b>Temporary.</b> Destroy when 3 years old, but longer retention is authorized if required for business use.</p>	<p>DAA-GRS-2016-00xx-0001</p>
020	<p><b>Key and card access accountability records.</b>  Records relating to accountability for keys issued.</p>	<p><b>Areas requiring highest level security awareness.</b>  Includes areas designated by the Interagency Security Committee as Facility Security Level V.</p> <p><b>Supersedes:</b>  GRS 18, item 16a (GRS 18, 1960, item 17)</p>	<p><b>Temporary.</b> Destroy 3 years after return of key, but longer retention is authorized if required for business use.</p>	<p>DAA-GRS-2016-00xx-0002</p>

Item	Records Description		Disposition Instruction	Disposition Authority
021		<p style="text-align: center;"><i>3 years</i></p> <p><b>All other facility security areas.</b> Includes areas designated by the Interagency Security Committee as Facility Security Levels I through IV.</p> <p><b>Supersedes:</b> GRS 18, item 16b (GRS 18, 1960, item 17) <i>6 months</i></p>	<p><b>Temporary.</b> Destroy 6 months after return of key, but longer retention is authorized if required for business use.</p>	<p>DAA-GRS-2016-00xx-0003</p>
030	<p><b>Uniform and equipment tracking records.</b> Records used to track the issuance of uniforms and equipment to security personnel including:</p> <ul style="list-style-type: none"> <li>• firearms (type, serial number, manufacturer, caliber, firearm registration date, storage location data, etc.)</li> <li>• communication devices issued to security personnel such as mobile radios and walkie-talkies</li> <li>• body armor such as bullet proof vests</li> <li>• police baton and holder</li> <li>• handcuffs and keys</li> </ul> <p><b>Supersedes:</b> GRS 18, item 19d (GRS 18, 1960, item 20d) <i>3 months</i></p>		<p><b>Temporary.</b> Destroy 3 months after return of equipment, but longer retention is authorized if required for business use.</p>	<p>DAA-GRS-2016-00xx-0004</p>
040	<p><b>Property pass records.</b> Records authorizing removal of government and privately owned property or materials off premises owned or leased by the Federal Government.</p> <p><b>Supersedes:</b> GRS 18, item 12 (GRS 18, 1960, item 13) <i>3 months</i></p>		<p><b>Temporary.</b> Destroy 3 months after expiration or revocation, but longer retention is authorized if required for business use.</p>	<p>DAA-GRS-2016-00xx-0005</p>
050	<p><b>Records of credit card abuse and postal irregularities.</b></p>		<p><b>Temporary.</b> Destroy 3 years</p>	<p>DAA-GRS-</p>

Item	Records Description	Disposition Instruction	Disposition Authority	
	<p>Records relating to irregularities in the handling of mail and the improper use or misuse of telephone calling cards and government charge or purchase cards. Includes:</p> <ul style="list-style-type: none"> <li>• postal irregularities reports such as loss or shortage of postage stamps or money orders, or loss or destruction of mail</li> <li>• semi-annual reports on government charge card violations</li> </ul> <p><b>Supersedes:</b> GRS 12, item 8 – in part (NC1-64-77-9, item 8) <i>3 years</i></p>	<p>after completion of investigation or when 3 years old, whichever is later, but longer retention is authorized if required for business use.</p>	<p>2016-00xx-0006</p>	
060	<p><b>Personally owned property accountability records.</b></p> <p>Records relating to accountability for non-government, personally owned property lost, abandoned, unclaimed, or believed stolen on premises owned or leased by the Federal government. Includes:</p> <ul style="list-style-type: none"> <li>• lost-and-found logs and release forms</li> <li>• loss statements</li> <li>• receipts</li> <li>• reports</li> </ul>	<p><b>Records for property valued over \$500.</b></p> <p>Records of unclaimed abandoned personal property retained for official use.</p> <p><b>Legal Citation:</b> 41 CFR 102-41.130</p> <p><b>Supersedes:</b> GRS 18, item 15a-in part (GRS 18, 1960, item 16a) <i>3 years</i> GRS 18, item 15b–in part(GRS 18, 1960, item 16b) <i>1 year</i></p>	<p><b>Temporary.</b> 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.</p>	<p>DAA-GRS-2016-00xx-0007</p>
061		<p><b>Records for property valued at \$500 or less.</b></p> <p>Records of unclaimed abandoned personal property not retained for official use.</p> <p><b>Legal citation:</b> 41 CFR 102-41.130</p> <p><b>Supersedes:</b> GRS 18, item 15a-in part (GRS 18, 1960, item 16a) <i>3 years</i> GRS 18, item 15b-in part (GRS 18, 1960, item</p>	<p><b>Temporary.</b> Destroy 30 days after the article is found, but longer retention is authorized if required for business use.</p>	<p>DAA-GRS-2016-00xx-0008</p>

Item	Records Description		Disposition Instruction	Disposition Authority
	16b) 1 year			
<b>Facility and physical security records.</b>				
070	<p><b>Interagency Security Committee member records.</b>                      Established by Executive Order 12977, the Department of Homeland Security (DHS) chairs the committee which provides leadership to the nonmilitary federal community supporting physical security programs. Records are agency copies of committee records documenting the administration, operation, and decisions of the committee. Includes:</p> <ul style="list-style-type: none"> <li>• agendas</li> <li>• meeting minutes</li> <li>• best practice and standards documents</li> <li>• funding documents for security countermeasures</li> </ul> <p><b>Excludes:</b> Records maintained by the Department of Homeland Security.</p> <p><b>Note:</b> See GRS 5.1 for internal committee records such as Facility Security Committee records.</p>		<b>Temporary.</b> Destroy when 10 years old, but longer retention is authorized if required for business use.	DAA-GRS-2016-00xx-0009
080	<p><b>Facility security assessment records.</b>                      Reports of survey and inspections of Government owned and privately owned facilities assigned security awareness by Government agencies conducted to ensure adequacy of protective and preventive measures taken against hazards of fire, explosion, and accidents; and to safeguard facilities against sabotage and unauthorized access. Includes:</p>	<p><b>Areas requiring highest level security awareness.</b>                      Includes areas designated by the Interagency Security Committee as Facility Security Level V.</p> <p><b>Supersedes:</b>                      GRS 18, item 9-in part (GRS 18, 1960, item 10) 3 years                      GRS 18, item 10-in part (GRS 18, 1960, item 11) 4 years</p>	<b>Temporary.</b> Destroy 5 years after security assessment has been updated or when security awareness has been terminated, whichever is sooner, but longer retention is authorized for business use.	DAA-GRS-2016-00xx-0010

Item	Records Description	Disposition Instruction	Disposition Authority
081	<ul style="list-style-type: none"> <li>• facility notes</li> <li>• inspector notes and reports</li> <li>• vulnerability assessments</li> </ul> <p><b>All other facility security areas.</b> Includes areas designated by the Interagency Security Committee as Facility Security Levels I through IV.</p> <p><b>Supersedes:</b> GRS 18, item 9-in part (GRS 18, 1960, item 10) <i>3 years</i> GRS 18, item 10-in part (GRS 18, 1960, item 11) <i>4 years</i></p>	<p><b>Temporary.</b> Destroy 3 years after security assessment has been updated or when security awareness has been terminated, whichever is sooner, but longer retention is authorized for business use.</p>	DAA-GRS-2016-00xx-0011
090	<p><b>Records of routine security operations.</b> Records used to detect potential security risks, threats, or prohibited items carried by visitors onto Federal property or impacting assets by providing access control, screening, patrol and response, and control center operations. Includes:</p> <ul style="list-style-type: none"> <li>• control center key or code records</li> <li>• registers of patrol and alarm services</li> <li>• service reports on interruptions and tests</li> <li>• emergency alarm contact call lists</li> <li>• temporary identification cards</li> <li>• round and perimeter check reports, including facility patrol tour data</li> <li>• surveillance records                             <ul style="list-style-type: none"> <li>○ recordings of protective mobile radio transmissions</li> <li>○ video surveillance recordings</li> <li>○ closed circuit television (CCTV) records</li> </ul> </li> <li>• door slip summaries</li> </ul> <p><b>Excludes:</b> Law enforcement officer-related records which are covered by agency-specific schedules.</p>	<p><b>Temporary.</b> Destroy when 30 days old, but longer retention is authorized if required for business use.</p>	DAA-GRS-2016-00xx-0012

Item	Records Description	Disposition Instruction	Disposition Authority
	<p><b>Note:</b> Records of accidents and incidents are covered under item 100 and records of visitor processing are covered under items 110 and 111.</p> <p><b>Supersedes:</b>            GRS 18, item 18a (GRS 18, 1960, item 19a) <i>1 year</i>            GRS 18, item 18b (GRS 18, 1960, item 19b) <i>1 month</i>            GRS 18, item 19a (GRS 18, 1960, item 20a) <i>superseded or obsolete</i>            GRS 18, item 19b (GRS 18, 1960, item 20b) <i>1 year</i>            GRS 18, item 19c (GRS 18, 1960, item 20c) <i>1 year</i>            GRS 21, item 11 (N1-GRS-98-2, item 37) <i>6 months</i>            GRS 21, item 18 (N1-GRS-98-2, item 39) <i>6 months</i></p>		
100	<p><b>Accident and incident records.</b>            Records of accidents and incidents involving Government owned or leased facilities, vehicles (land, water, and air), and property used by Federal agencies. Includes:</p> <ul style="list-style-type: none"> <li>• statements of witnesses</li> <li>• warning notices</li> <li>• records relating to arrests, commitments, and traffic violations</li> <li>• accident and incident reports</li> <li>• law enforcement agency requests for information</li> </ul> <p><b>Excludes:</b> Records of the Federal Aviation Administration and the National Transportation Safety Board relating to aircraft used by Federal agencies, including leased aircraft used by Federal agencies.</p> <p><b>Supersedes:</b>            GRS 10, item 13 (N1-GRS-04-6, item 5) <i>1 year after completion of investigation</i>            GRS 18, item 11 (GRS 18, 1960, item 12) <i>2 years</i></p>	<p><b>Temporary.</b> Destroy 3 years after final investigation or reporting action or when 3 years old, whichever is later, but longer retention is authorized for business use.</p>	DAA-GRS-2016-00xx-0013

Item	Records Description	Disposition Instruction	Disposition Authority	
	<p>GRS 18, item 14a (GRS 18, 1960, item 15a) <i>3 years</i></p> <p>GRS 18, item 14b (GRS 18, 1960, item 15b) <i>2 years</i></p> <p>GRS 18, item 14c (GRS 18, 1960, item 15c) <i>1 years</i></p>			
110	<p><b>Visitor processing records.</b> Registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on vehicles and passengers.</p>	<p><b>Areas requiring highest level security awareness.</b> Includes areas designated by the Interagency Security Committee as Facility Security Level V.</p> <p><b>Supersedes:</b> GRS 18, item 17a (GRS 18, 1960, item 18) <i>5 years</i> GRS 18, item 20a-in part (GRS 18, 1960, item 21a) <i>2 years</i> GRS 18, item 20b-in part (GRS 18, 1960, item 21b) <i>1 year</i></p>	<p><b>Temporary.</b> Destroy when 5 years old, but longer retention is authorized if required for business use.</p>	DAA-GRS-2016-00xx-0014
111		<p><b>All other facility security areas.</b> Includes areas designated by the Interagency Security Committee as Facility Security Levels I through IV.</p> <p><b>Supersedes:</b> GRS 18, item 17b (GRS 18, 1960, item 18) <i>2 years</i> GRS 18, item 20a-in part (GRS 18, 1960, item 21a) <i>2 years</i> GRS 18, item 20b-in part (GRS 18, 1960, item 21b) <i>1 year</i></p>	<p><b>Temporary.</b> Destroy when 3 years old, but longer retention is authorized if required for business use.</p>	DAA-GRS-2016-00xx-0015



Item	Records Description		Disposition Instruction	Disposition Authority
120	<p><b>Personal identification verification credentials and cards.</b> Records related to credential badges (such as smart cards) used to access buildings and systems that are identity verified and meet standards for identification issued to Federal employees, contractors, and dependents in gaining physical access to controlled facilities and logical access to controlled information systems. Also referred to as Common Access Cards (CAC) cards, Personal Identification Verification (PIV) Cards, and Homeland Security Presidential Directive 12 (HSPD-12) Program credentials.</p> <p><b>Excludes:</b> PIV records of certain classes of government employees, such as those covered under special-risk security provisions or 44 U.S.C Section 3542, should be scheduled separately by agencies.</p>	<p><b>Application and activation records.</b> Applications and supporting documentation, such as chain-of-trust records, for identification credentials. Includes:</p> <ul style="list-style-type: none"> <li>• application for identification card</li> <li>• 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.</li> <li>• lost or stolen credential documentation or police report</li> </ul> <p><b>Note:</b> Applications for access to information systems are retained under GRS 3.2 Information Systems Security Records.</p> <p><b>Supersedes:</b> GRS 11, item 4a in part (GRS 11, 1952, item 4a – in part) <i>3 months after return</i> GRS 11, item 4b in part (GRS 11, 1952, item 4b – in part) <i>destroy after accounted for</i> GRS 21, item 2 in part (N1-GRS-98-2, item 33 – in part) <i>5 years</i></p>	<p><b>Temporary.</b> Destroy when 5 years old or after deactivation or confiscation of credential, whichever is sooner, but longer retention is authorized if required for business use.</p>	DAA-GRS-2016-00xx-0016
121		<p><b>Cards.</b></p>		
130	<p><b>Local facility identification and card access records.</b> Identification verification credentials issued by facility or building managers to provide local</p>		<p><b>Temporary.</b> Destroy 3 months after credential is</p>	DAA-GRS-2016-00xx-

Item	Records Description	Disposition Instruction	Disposition Authority
	<p>identification and access. Includes:</p> <ul style="list-style-type: none"> <li>• temporary identification badges for interns serving less than 180 days</li> <li>• supplemental badges issued to access elevators</li> <li>• personnel identification photographs</li> <li>• parking permits</li> </ul> <p><b>Supersedes:</b>            GRS 11, item 4a in part (GRS 11, 1952, item 4a – in part) <i>3 months after return</i>            GRS 11, item 4b in part (GRS 11, 1952, item 4b- in part) <i>destroy after accounted for</i>            GRS 21, item 2 in part (N1-GRS-98-2, item 33 – in part) <i>5 years</i></p>	<p>renewed or 3 months after individual no longer requires access, whichever is sooner, but longer retention is authorized for business use.</p>	<p>0018</p>
140	<p><b>Sensitive Compartmented Information Facility (SCIF) accreditation records.</b>            Physical security preconstruction plans for SCIF construction, expansion or modification. Includes:</p> <ul style="list-style-type: none"> <li>• Fixed Facility Checklist</li> <li>• pre-accreditation inspection report</li> </ul>	<p><b>Temporary.</b> Destroy when SCIF receives final accreditation, but longer retention is authorized if required for business use.</p>	<p>DAA-GRS-2016-00xx-0019</p>
150	<p><b>Sensitive Compartmented Information Facility (SCIF) inspection records.</b>            Inspection records required by Intelligence Community Directive (ICD) 705. Includes:</p> <ul style="list-style-type: none"> <li>• Fixed Facility Checklist</li> <li>• accreditation authorization documents</li> <li>• inspection reports, including Technical Surveillance Counter Measures (TCSM) reports, for the entire period of SCIF accreditation</li> <li>• operating procedures</li> <li>• Special Security Officer Contractor Special Security Officer (SSO/CSSO) appointment letters</li> <li>• memoranda of agreements (MOAs)</li> <li>• Emergency Action Plans</li> <li>• copies of any waivers granted by the Cognizant Security Authority (CSA)</li> </ul>	<p><b>Temporary.</b> Destroy when 5 years old or after SCIF has been de-accredited for longer than one year, but longer retention is authorized if required for business use.</p>	<p>DAA-GRS-2016-00xx-0020</p>

Item	Records Description		Disposition Instruction	Disposition Authority
160	<p><b>Canine (K-9) service records.</b> Records document the acquisition, training, activities, care, and retirement of canine partners of police officers. Includes:</p> <ul style="list-style-type: none"> <li>• acquisition records</li> <li>• breeder and lineage records</li> <li>• vaccination and medical history records</li> <li>• microchip number and identification records</li> <li>• deficiencies/remedies</li> <li>• training courses taken and resulting grades and certifications</li> <li>• initial report of positive detections and bite incidents</li> <li>• end-of-service documentation (through retirement or death)</li> </ul>		<p><b>Temporary.</b> Destroy 3 years after dog is released from service or when superseded or obsolete, whichever is sooner, but longer retention is authorized if required for business use.</p>	DAA-GRS-2016-00xx-0021
<b>Personnel security clearance records.</b>				
170	<p><b>Personnel security clearance investigative reports.</b> Investigative reports and related documents used and/or created by agencies to conduct security/suitability determinations and issue security clearances. Also referred to as Fitness For Duty or pre-employment screening records.</p>	<p><b>Reports provided by external investigative organizations.</b></p> <p><b>Supersedes:</b> GRS 18, item 22b (NC1-GRS-80-1 item 23b) <i>Destroy in accordance with the investigating agency instruction</i></p>	<p><b>Temporary.</b> Destroy in accordance with the investigating agency instructions.</p>	DAA-GRS-2016-00xx-0022
171		<p><b>Reports created by agencies conducting investigations under delegated investigative authority.</b></p>	<p><b>Temporary.</b> Destroy in accordance with delegated authority agreement or memorandum of understanding.</p>	DAA-GRS-2016-00xx-0023

Item	Records Description		Disposition Instruction	Disposition Authority	
180	<p><b>Personnel security and access clearance records.</b> Records of processing security clearances and other clearances for access to Government facilities or to sensitive data. Includes:</p> <ul style="list-style-type: none"> <li>• questionnaires</li> <li>• summaries of reports prepared by the investigating agency</li> <li>• documentation of agency adjudication process and final determination</li> </ul> <p><b>Note:</b> Information system access records are covered by GRS 3.2, items 030 and 031.</p>		<p><b>Records of persons not issued clearances.</b> Includes case files of applicants not hired and those given unfavorable determination decisions.</p>	<p><b>Temporary.</b> Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use.</p>	DAA-GRS-2016-00xx-0024
181	<p><b>Records of persons issued clearances.</b></p> <p><b>Excludes:</b> Copies of investigative reports covered in items 170 and 171.</p> <p><b>Supersedes:</b> GRS 18, item 22a (NC1-GRS-80-1, item 23a) 5 years</p>		<p><b>Temporary.</b> Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use.</p>	DAA-GRS-2016-00xx-0025	
190	<p><b>Personnel security and access clearance status records.</b> Lists or rosters showing the current security clearance status of individuals.</p> <p><b>Supersedes:</b> GRS 18, item 22c (NC1-GRS-80-1, item 23c) <i>Destroy with related case file</i> GRS 18, item 23 (NC1-GRS-80-1, item 24) <i>when superseded or obsolete</i></p>		<p><b>Temporary.</b> Destroy when superseded or obsolete.</p>	DAA-GRS-2016-00xx-0026	
200	<p><b>Information security violations records.</b> Case files relating to investigations of alleged violations of Executive orders, laws, or agency regulations for the safeguarding of national security information.</p>	<p><b>Cases referred to investigative agencies.</b> Files relating to alleged violations referred to the Department of Justice or Department of Defense.</p> <p><b>Supersedes:</b> GRS 18, item 24a (NC1-GRS-81-8, item 1a) 5 years</p>	<p><b>Temporary.</b> Destroy 5 years after close of case, but longer retention is authorized if required for business use.</p>	DAA-GRS-2016-00xx-0027	
201		<p><b>All other cases.</b> Includes final reports and products.</p>	<p><b>Temporary.</b> Destroy 2 years after completion of final</p>	DAA-GRS-2016-00xx-	

Item	Records Description		Disposition Instruction	Disposition Authority
	<p>Includes final reports and products.</p> <p><b>Excludes:</b> Documents placed in Official Personnel Folders.</p>	<p><b>Supersedes:</b> GRS 18, item 24b (N1-GRS-98-2, item 31) 2 years</p>	<p>action, but longer retention is authorized if required for business use.</p>	<p>0028</p>
<b>Insider threat protection records.</b>				
210	<p><b>Insider threat protection administrative and operations records.</b> Records related to program and planning of insider threat activities. Includes:</p> <ul style="list-style-type: none"> <li>• correspondence related to data gathering</li> <li>• briefing materials and presentations</li> <li>• status reports</li> <li>• procedures, operational manuals, and related development records</li> <li>• implementation guidance</li> <li>• plans or directives and supporting documentation, such as:                             <ul style="list-style-type: none"> <li>○ independent and self-assessments</li> <li>○ corrective action plans</li> <li>○ evaluative reports</li> </ul> </li> </ul> <p><b>Exclusion:</b> This item does not include the records of the “Senior Agency Official” as defined in E.O. 13526, section 5.4 (d).</p> <p><b>Note:</b> Records related to employee training are scheduled in GRS 2.6.</p>		<p><b>Temporary.</b> Destroy when 7 years old, but longer retention is authorized if required for business use.</p>	<p>DAA-GRS-2016-00xx-0029</p>
220	<p><b>Insider threat protection inquiry records.</b> Records related to the non-investigative, administrative process of trend analysis or data analytics generated by the ITP program or function. Includes the case-specific final reports and associated data collection which lead to case referrals to the appropriate investigative entity. Includes:</p> <ul style="list-style-type: none"> <li>• queries and associated data collection</li> </ul>		<p><b>Temporary.</b> Destroy 7 years after case referral has been made or after 7 years of inactivity subject to review, but longer retention is</p>	<p>DAA-GRS-2016-00xx-0030</p>

Item	Records Description	Disposition Instruction	Disposition Authority
	<ul style="list-style-type: none"> <li>• statistics</li> <li>• final reports</li> </ul> <p><b>Exclusion:</b> Records of the subsequent investigations are covered under other agency-specific schedules, such as Office of the Inspector General schedules.</p>	authorized if required for business use.	
230	<p><b>Insider threat protection data collection.</b></p> <p>Data collection maintained by agencies undertaking analytic and risk-based data collection activities to implement insider threat directives and standards directed by E.O. 13587. Agency ITP offices or functions gather and integrate information to conduct a preliminary review of any potential insider threat issues. Identified threats are referred to the Department of Justice, the Office of Inspector General, security office, information assurance office, human resources office, or to the proper law enforcement authority. Includes copies of:</p> <ul style="list-style-type: none"> <li>• personnel data and administrative actions</li> <li>• personnel security files, including security incident or violation files</li> <li>• facility access records, including visitor records</li> <li>• information technology access records, including network security records</li> <li>• investigatory records, including statements of complainants, informants, suspects, and witnesses</li> <li>• travel records, including foreign visitor or contact reports</li> <li>• financial records, including financial disclosure reports</li> <li>• public records, including court records</li> <li>• law enforcement records</li> <li>• personal biographical and identification data, including U.S. Government name check data</li> <li>• generic open source and social media data</li> <li>• communications data</li> <li>• referral records</li> </ul>	<b>Temporary.</b> Destroy when 25 years old or when business use ceases, whichever is sooner.	DAA-GRS-2016-00xx-0031

Item	Records Description	Disposition Instruction	Disposition Authority
	<ul style="list-style-type: none"><li>• intelligence records</li><li>• Agency or Bureau Department data</li><li>• private industry data</li></ul>		



NATIONAL ARCHIVES *and*  
RECORDS ADMINISTRATION  
8601 ADELPHI ROAD  
COLLEGE PARK, MD 20740-6001  
[www.archives.gov](http://www.archives.gov)

**Date:** April 15, 2016  
**Appraiser:** Laura Adams McHale, ACRA  
**Agency:** General Records Schedules (GRS)  
**Subject:** DAA-GRS-2016-000X (schedule not entered into ERA)      **DRAFT**

## **INTRODUCTION**

### **Schedule Overview**

GRS 5.6: Security Records

### **Additional Background Information**

This schedule provides disposition authority for records related to the function of managing the protection of an organization's personnel, assets, and facilities. It supersedes 46 items found throughout old GRS 10, 11, 12, 18, and 21.

This schedule aggregates the law enforcement function, referred to as "police functions" in old GRS 18, into an item for routine security operations records (schedule item no. 090).

We added 10 new items to this schedule:

Schedule item no. 070, Interagency Security Committee member records

Schedule item no. 121, Personal identification verification credentials and cards-cards

Schedule item no. 140, Sensitive Compartmented Information Facility (SCIF) accreditation records

Schedule item no. 150, Sensitive Compartmented Information Facility (SCIF) inspection records.

Schedule item no. 160, Canine (K-9) service records

Schedule item no. 171, Personnel security clearance investigative reports- Reports created by agencies conducting investigations under delegated investigative authority

Schedule item no. 180, Personnel security and access clearance records- Records of persons not issued clearances

Schedule item no. 210, Insider threat protection administrative and operations records

Schedule item no. 220, Insider threat protection inquiry records

Schedule item no. 230, Insider threat protection data collection

Forty-seven agency subject matter experts (SMEs) assisted in the development of this schedule by participating in 3 subgroups organized into categories of personnel security, physical security, and insider threat protection.

### **Overall Recommendation**



I recommend approval of the attached schedule.

## **APPRAISAL**

### **Item 0001 (GRS 5.6, item 010): Security administrative records.**

This item covers routine administrative records created and maintained by agency security programs.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

#### **Appraisal Justification:**

\* Previously approved as temporary.

GRS 18, item 8 (GRS 18, 1960, item 9)

GRS 18, item 13a (GRS 18, 1960, item 14a)

GRS 18, item 13b (GRS 18, 1960, item 14b)

GRS 18, item 21 (NC1-GRS-80-1, item 22)

\* Has little or no research value. Records are administrative in nature. The records covered under this item are associated with day-to-day administrative and/or routine activities.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. This item increases the retention of three previously-approved GRS items from 2 to 3 years in response to a growing consensus in the Federal records community that records documenting general administrative activity should be retained for 3 years. The items being increased from 2 to 3 years are: GRS 18, item 8, Security and Protective Services Administrative Correspondence Files (GRS 18, 1960, item 9); GRS 18, item 13b, Guard Assignment Files-Requests, analyses, reports, change notices, and other papers relating to post assignments and strength requirements (GRS 18, 1960, item 14b); and GRS 18, item 21, Security Clearance Administrative Subject Files (NC1-GRS-80-1, item 22). GRS 18, item 13a, Guard Assignment Files-Ledger Records (GRS 18, 1960, item 14a) were previously retained for 3 years; the retention remains unchanged.

These records should be retained for at least a minimum of 3 years to ensure adequate and proper documentation of the actions and transactions of the federal government. Agencies are authorized to keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

### **Item 0002 (GRS 5.6, item 020): Key and card access accountability records-Areas requiring highest level security awareness.**

### **Item 0003 (GRS 5.6, item 021): Key and card access accountability records-All other facility security areas.**

Both items supersede old GRS items for key control records which now includes records generated by key card access devices. The description has been updated to reflect facility security level descriptions established by the Interagency Security Committee (ISC).

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

#### **Appraisal Justification:**

\* Previously approved as temporary.

GRS 18, item 16a (GRS 18, 1960, item 17)

GRS 18, item 16b (GRS 18, 1960, item 17)

\* Has little or no research value. Records are administrative in nature.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. Key audits are conducted at Level III Federal Facilities (as defined by the ISC) and above, every 3 years; Level II Federal Facilities and below, every 5 years. The retention of both items is unchanged as the retention periods established in 1960 still meet business needs for the records. Agencies are authorized to keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0004 (GRS 5.6, item 030): Uniform and equipment tracking records.**

This item expands an existing item used to track firearms to cover an administrative need to track Government-issued uniforms and other equipment.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 18, item 19d (GRS 18, 1960, item 20d)

\* Has little or no research value. Records are administrative in nature.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. The retention is unchanged as the retention period established in 1960 still meets agency business needs for the records. Agencies are authorized to keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0005 (GRS 5.6, item 040): Property pass records.**

This item covers routine administrative records used to signify to security guards that removal of property is authorized by the organization for whom the property is considered accountable.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 18, item 12 (GRS 18, 1960, item 13)

\* Has little or no research value. Records are administrative in nature.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. The retention is unchanged as the retention period established in 1960 still meets agency business needs for the records. Agencies are authorized to keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0006 (GRS 5.6, item 050): Records of credit card abuse and postal irregularities.**

This item provides disposition authority for administrative records documenting postal, telephone calling card, and/or credit or purchase card misuse. While not theft, misuse constitutes improper use or a violation of established procedures and results in an investigation of internal controls.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary. GRS 12, item 8 – in part (NC1-64-77-9, item 8-in part). This item is partially superseded to address security and investigatory needs for the records in this GRS. The other portion of this item is addressed by GRS 5.5, item 020. The mail service’s reason for keeping the records for "reports of loss, rifling, delayed or late delivery, wrong delivery, or other improper treatment of mail" differs from the security office’s reason for keeping the records. GRS 5.5, item 020 has a shorter, 1-year retention period.

\* Has little or no research value. Records are administrative in nature.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. The retention period is unchanged. Agencies are authorized to keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0007 (GRS 5.6, item 060): Personally owned property accountability records - Records for property valued over \$500.**

**Item 0008 (GRS 5.6, item 061): Personally owned property accountability records - Records for property valued at \$500 or less.**

Both items cover records used to document personal property that is lost, abandoned, unclaimed, or believed stolen on premises owned or leased by the Federal Government. The items have been updated in title and description to clarify records are for non-government, personally owned property as opposed to real property.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 18, item 15a (GRS 18, 1960, item 16a)

GRS 18, item 15b (GRS 18, 1960, item 16b)

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. The new items are divided according to property being valued over or under \$500 because agencies must hold all unclaimed personal property for 30 days until title vests in the Government. Documentation of personal property valued over \$500, which is then retained by the agency for official use, must be kept for an additional 3 years from the date that title to the property vests in the Government in order to allow time for the former owner to file a claim. While agencies may keep records of all unclaimed personally owned property for 3 years, most lost-and-found documentation may be safely disposed 30 days after an article is found. Adding these two new items to the GRS provides a shorter retention period for the vast majority of lost-and-found documentation associated with routine security operations.

As a result, we mapped the old GRS 18, item 15a, Ledger Records to both new GRS items (which is why the old items are superseded in part) because agencies may keep different tracking logs for lost-and-found articles, although this is not a requirement. We also mapped to both new items the old GRS 18, item 15b, Personal Property Accountability Files-Reports, loss statements, receipts, and other documents relating to lost and found articles. Documents and receipts for property valued over \$500 must be kept for 3 years and similar records for property under \$500 are kept for 30 days after being found. Agencies may keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0009 (GRS 5.6, item 070): Interagency Security Committee member records.**

This item covers the records of agency participation in the Interagency Security Committee (ISC).

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Captured elsewhere in permanent records. NARA Job No. N1-563-08-6, item 2a, Inter-agency Committees- Records documenting the committee's and all subcommittees' establishment, organization, policy, membership, meetings, findings, recommendations, and accomplishments. ISC records at the Department of Homeland Security are scheduled as permanent.

\* Similar records have been approved as temporary. NARA Job No. N1-563-08-6, item 2b. Inter-agency Committees-All Other Copies, specifically addressed the temporary value of the Department of Homeland Security's ISC records relating to the logistical aspects of meetings and hearings, general technical analyses written to inform a broad audience about promising technologies, such as technical notes and technical information bulletins, and fact sheets.

\* Has little or no research value. Records are administrative in nature.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. A minimum retention period of 10 years is recommended by the Department of Homeland Security's Interagency Security Committee in *Facility Security Committees* (2<sup>nd</sup> Edition, January 1, 2012), page 22. Agencies are authorized to keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0010 (GRS 5.6, item 080): Facility security assessment records - Areas requiring highest level security awareness.**

**Item 0011 (GRS 5.6, item 081): Facility security assessment records - All other facility security areas.**

These items cover records needed to conduct facility security assessments according to the standards and timeframes established by the Interagency Security Committee (ISC). Records include inspector notes, reports, and vulnerability assessments.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 18, item 9 (GRS 18, 1960, item 10)

GRS 18, item 10 (GRS 18, 1960, item 11)

\* Has little or no research value. Records are administrative in nature.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. This item combines the former Survey and Inspection Files covered by GRS 18, item 9 and item 10. GRS 18, item 9 scheduled inspections of government facilities for 3 years and GRS 18, item 10 scheduled inspections of privately-owned facilities for 4 years. We removed the distinction between the retention of government owned and privately owned

facilities because there is no business reason today for this separation which is why the old items are superseded in part and mapped to each of the new items. We altered the retention periods to 3 and 5 years to correspond to the ISC facility security level timeline for conducting surveys and inspections. The facilities designated with the highest facility security levels are surveyed every 3 years and the facilities with lower security levels are surveyed every 5 years. Agencies may keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0012 (GRS 5.6, item 090): Records of routine security operations.**

This item covers routine operational records created and maintained through the 5 basic security functions of access control, screening, patrol and response, and control center operations. 1 Visitor processing, the sixth basic security function identified by the Interagency Security Committee, is covered by item nos. 110 and 111 of this schedule.

At the time of GRS 18's issuance in 1952, the General Services Administration (GSA) had recently gained responsibility for the functions of the Federal Works Agency (FWA). When Congress established the FWA in 1948, it empowered the Federal Works Administrator to:

appoint uniformed guards as special policemen with the responsibility of "the policing of public buildings and other areas under the jurisdiction of the Federal Works Agency." The special policemen were given the same responsibility as sheriffs and constables on federal property to enforce the laws enacted for the protection of persons and property, and to prevent "breaches of peace, suppress affrays or unlawful assemblies."<sup>2</sup>

After the establishment of the Federal Protective Service (FPS) in 1971, GSA uniformed officers retained the right to make arrests for offenses committed on federal property. Passage of the Homeland Security Act of 2002 (P.L. 107-296) resulted in the transfer of FPS to the newly formed Department of Homeland Security (DHS), under U.S. Immigration and Customs Enforcement (ICE). FPS is currently in the National Protection and Programs Directorate of DHS.

Why does this matter? Today's physical security of federal facilities is provided by contract armed security officers (ASOs) who do not conduct law enforcement functions and are not police. The Interagency Security Committee defines an ASO as: "a member of a facility security force and an element of a security post who is issued a firearm and has the training, equipment, and appropriate certifications to perform security functions."<sup>3</sup> GRS 5.6 covers the security functions of access control, screening, visitor processing, patrol and response, and control center operations.

As a result, we have added the old GRS items for Police Functions Files (GRS 18, items 14a-c) to a new item for routine security operations records. While there remains a cadre of FPS law enforcement officers (LEOs), law enforcement activities are not covered by GRS 5.6 and are scheduled by agencies with law enforcement activities as a mission focus. Examples of

---

1 *Best Practices for Armed Security Officers in Federal Facilities* (Interagency Security Committee, 2<sup>nd</sup> edition, April 2013).

2 Order Code RS22706, Shawn Reese. *The Federal Protective Service and Contract Security Guards: A Statutory History and Current Status* (Congressional Research Service, Updated February 11, 2008), page CRS-1.

3 Interagency Security Committee, *Best Practices for Armed Security Offices in Federal Facilities* (2<sup>nd</sup> Edition, April 2013), page 3.

agencies which operate police forces in their own specialized jurisdictions include not only the FPS but, the Postal Police, the Park Police, the U.S. Secret Service, the U.S. Marshals Service, Amtrak Police, and others.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 18, item 18a (GRS 18, 1960, item 19a) *1 year*

GRS 18, item 18b (GRS 18, 1960, item 19b) *1 month*

GRS 18, item 19a (GRS 18, 1960, item 20a) *superseded or obsolete*

GRS 18, item 19b (GRS 18, 1960, item 20b) *1 year*

GRS 18, item 19c (GRS 18, 1960, item 20c) *1 year*

GRS 21, item 11 (N1-GRS-98-2, item 37) *6 months*

GRS 21, item 18 (N1-GRS-98-2, item 39) *6 months*

\* Has little or no research value. Records are administrative in nature.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. The retention period of old GRS 10, item 18b, Facilities Checks Files remains unchanged. This item reduces the retention of Facilities Checks Files (GRS 18, item 18a) and Guard Service Control Files (GRS 18, items 19b and 19c) from 1 year to 30 days because these are routine operations records generated by agencies which have a short term temporary, albeit important, business value. Similarly, Routine Surveillance Footage (GRS 21, item 11) and Routine Surveillance Recordings (GRS 21, item 18) are reduced from a 6-month to a 30 day retention period to meet minimum operational requirements.

A review of previously approved schedules indicated some agencies had schedules for retention periods of 14-days for routine surveillance records; however, most of these schedules were at least 5-years old and we believe current technology now readily enables a 30-day retention period. An additional reason for keeping routine surveillance records at least 30 days is to meet the needs of local law enforcement agencies which request agency copies of surveillance footage. Since more significant security operational records of accidents and incidents, as well as visitor processing, are kept for longer periods of time per item 100 of this schedule, this item's lower retention period meets agency business needs as well as minimum legal requirements. Agencies are authorized to keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0013 (GRS 5.6, item 100): Accident and incident records.**

This item provides disposition authority for the case files set up as part of an agency's response to accidents and incidents involving Government owned or leased facilities, vehicles (land, water, and air), and property.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 10, item 13 (N1-GRS-04-6, item 5) *1 year after completion of investigation*

GRS 18, item 11 (GRS 18, 1960, item 12) *2 years*

GRS 18, item 14a (GRS 18, 1960, item 15a) *3 years*

GRS 18, item 14b (GRS 18, 1960, item 15b) *2 years*

GRS 18, item 14c (GRS 18, 1960, item 15c) *1 years*

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. This item is an aggregation of several old GRS items. We identified a 3-year after completion of investigation retention period because a 3-year retention best reflects current practices for administrative records as opposed to the other items from 1960. The value of these records lies in the agency-provided copy of the underlying documentation of the incident which leads to case referral. An agency's security function has a safeguarding focus and is not responsible for crime investigation. If criminal activity is suspected, agencies refer such matters to other agencies with investigative jurisdiction or local law enforcement. As a result, the agency copy has a short-term, limited business use as it forms part of an investigative case file held by other agencies. Agencies are authorized to keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0014 (GRS 5.6, item 110): Visitor processing records- Areas requiring highest level security awareness.**

**Item 0015 (GRS 5.6, item 111): Visitor processing records- All other facility security areas.**

These items provide disposition authority for records created when visitors enter Federal facilities and properties. This new item combines old GRS 18, items 17a-b, Visitor Control Files with old GRS 18, items 20a-b, Logs and Registers because all four items cover related visitor's records. GRS 18, items 20a-b are covered in part because there are now two categories for the records depending on facility security level whereas in the past GRS there was only one corresponding GRS item.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 18, item 17a (GRS 18, 1960, item 18) *5 years*

GRS 18, item 17b (GRS 18, 1960, item 18) *2 years*

GRS 18, item 20a (GRS 18, 1960, item 21a) *2 years*

GRS 18, item 20b (GRS 18, 1960, item 21b) *1 year*

\* Has little or no research value. Records are administrative in nature. The records covered under this item are associated with non-supervisory, administrative and/or routine activities.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. The 5-year retention period for visitor logs of high security areas (GRS 18, item 17a) is unchanged. The retention period of visitor's logs for all other security areas has been increased from 2 to 3 years to correspond with the Interagency Security Committee's facility security level timeline for conducting surveys and inspections. The facilities designated with the highest facility security levels are surveyed every 3 years and the facilities with lower security levels are surveyed every 5 years. Agencies may keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0016 (GRS 5.6, item 120): Personal identification verification credentials and cards- Application and activation records.**

**Item 0017 (GRS 5.6, item 121): Personal identification verification credentials and cards- Cards.**

These items provide disposition authority for the applications, activation records, and physical cards issued following the guidelines of the Homeland Security Presidential Directive 12 (HSPD-12) Programs operated by agencies. HSPD-12 specified a *Policy for a Common Identification Standard for Federal Employees and Contractors*. Following the issuance of HSPD-12, the National Institute of Standards and Technology (NIST) Computer Security Division developed and issued Federal Information Processing Standard (FIPS) 201, titled *Personal Identity Verification of Federal Employees and Contractors*, on February 25, 2005.<sup>4</sup> All federal departments and agencies and all their contractors requiring access to federal facilities and systems must comply with the standard and the specifications of FIPS 201, except that the standard shall not apply to identification associated with national security systems as defined by law and exempted through 44 U.S.C. Section 3542(b)(2) (reference 1). Also exempt are special-risk security provisions, as defined in FIPS 201-1 (reference 2).<sup>5</sup>

The significance of the HSPD-12 Program is that there is now a common policy being followed throughout the Federal Government; the records are mostly electronic; and the records now bundle personal and biometric data about individuals. There is no centralized collection point or information system gathering this data within the Government. Agencies operate or contract for PIV services via shared services mechanisms.

The PIV cards are disposable under item 121. Though it's debatable whether the physical identification badge meets the criteria of a Federal record, we added an item to provide a definitive disposal authority for the cards.

This new GRS provides a separate category under item no. 130, Local facility identification and card access records which is why all of the older GRS items (listed below) related to identification badges are superseded in part and mapped to multiple item categories; there are now two categories of identification badges when there used to be one in other words.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 11, item 4a in part (GRS 11, 1952, item 4a – in part) *3 months after return*

GRS 11, item 4b in part (GRS 11, 1952, item 4b- in part) *destroy after accounted for*

GRS 21, item 2 (N1-GRS-98-2, item 33 – in part) *5 years*

\* Has little or no research value. Records are administrative in nature. The records covered under this item are associated with non-supervisory, administrative and/or routine activities.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. Identification credentials have been scheduled as temporary records by GRS 11, items 4a and 4b since 1952. Retention is being changed from 3 months after credential's return

---

4 *About Personal Identity Verification (PIV) of Federal Employees and Contractors* posted at <http://csrc.nist.gov/groups/SNS/piv/> and accessed on March 7, 2016. In August 2013, NIST issued FIPS-201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*.

5 *FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors* posted at <http://csrc.nist.gov/groups/SNS/piv/npivp/FIPS201FAQ.htm> and accessed on March 7, 2016.



(GRS 11, item 4a) to when 5 years old because this is the length of time a PIV card is valid before it requires reactivation. GRS 21, item 2 provided for a 5-year retention of personnel photographs and this remains unchanged. Agencies may keep records longer if they have a business need to do so. The cards themselves may be destroyed, following special handling procedures, once expired or revoked.

**Media Neutrality:** Approved

**Item 0018 (GRS 5.6, item 130): Local facility identification and card access records.**

This item provides disposition authority for credentials issued by local building managers needed by persons, such as interns, requiring short-term building access or by staff to access elevators, floors, and other resources not accessed via the HSPD-12 issued PIV credentials. This new GRS provides a separate category under item nos. 120 and 121, Personal identification verification credentials and cards which is why all of the older GRS items (listed below) related to identification badges are superseded in part and mapped to multiple item categories; there are now two categories of identification badges when there used to be one in other words.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 11, item 4a in part (GRS 11, 1952, item 4a – in part) *3 months after return*

GRS 11, item 4b in part (GRS 11, 1952, item 4b- in part) *destroy after accounted for*

GRS 21, item 2 in part (N1-GRS-98-2, item 33 – in part) *5 years*

\* Has little or no research value. Records are administrative in nature. The records covered under this item are associated with non-supervisory, administrative and/or routine activities.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. Several old GRS items are superseded in part and mapped to these items because the old GRS only had 1 category of identification badges and now there are two. As the Government moves towards a common policy for identification, this local identification badge category may no longer be needed going forward. However, there are still requirements today for short term badges for which this item provides disposition authority.

The retention of the existing item, GRS 11, item 4a, is unchanged. The other two items, GRS 11, item 4b and GRS 21, item 2, are aggregated as part of this item to provide a unified retention period for the records. GRS 11, item 4b had a previous retention period of “Destroy after all listed credentials are accounted for.” These associated receipts will now be disposable at the same time as the credential which meets agency business needs for the records. GRS 21, item 2 is superseded in part because it is mapped to this item to cover the “personnel photographs” portion of the old item; the passport photographs portion is mapped elsewhere. Its retention is lowered from 5 years to 3 months because there is no business use for the photographs outside of the need to generate a local identification badge. Agencies may keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0019 (GRS 5.6, item 140): Sensitive Compartmented Information Facility (SCIF) accreditation records.**

This item provides disposition authority for records concerning the physical security pre-construction plans required to support SCIF accreditation following the standards and best practices established by Intelligence Community Directive (ICD) 705, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities (ICS-705-1)* and *Standards for Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities (ICS-705-2)*.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\*Similar records have been proposed for temporary retention. Sensitive Compartmented Information (SCI) billet files, N1-AU-99-12, item 1.

\* Has little or no research value. Records are administrative in nature.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. Intelligence Community Directive (ICD) 705 requires all SCIF's be built to a standard recognized and accepted by all intelligence community agencies. Once the SCIF has received final accreditation there is no need to maintain pre-construction review files. Agencies may keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0020 (GRS 5.6, item 150): Sensitive Compartmented Information Facility (SCIF) inspection records.**

This item concerns inspection records kept by agencies following the standards and best practices established by Intelligence Community Directive (ICD) 705, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities (ICS-705-1)* and *Standards for Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities (ICS-705-2)*.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Similar records have been proposed for temporary retention. Sensitive Compartmented Information Facility (SCIF) accreditations and physical security file, N1-AU-99-12, item 3.

\*Has little or no research value. Records are administrative in nature.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. ICD 705 requires the re-inspection of SCIFs every 5 years. ICD 705 also allows re-accreditation of a de-accredited SCIF at the previous accreditation level within 1 year of the SCIF's de-accreditation. Longer retention may be necessary based on limited resources to conduct SCIF inspections. Agencies may keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0021 (GRS 5.6, item 160): Canine (K-9) service records.**

This item provides disposition authority for records documenting canine (K-9) service.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Similar records have been approved as temporary. Police K9 (Canine) Files, DAA-0537-2014-0004-0001.

\* Has little or no research value. Records are administrative in nature. The records covered under this item are associated with non-supervisory, administrative and/or routine activities.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. The retention period of 3 years after service retirement is similar to the retention of other routine administrative records. Agencies may keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 022 (GRS 5.6, item 170): Personnel security clearance investigative reports- Reports provided by external investigative organizations.**

**Item 023 (GRS 5.6, item 171): Personnel security clearance investigative reports- Reports created by agencies conducting investigations under delegated investigative authority.**

These items provide disposition authority for investigative reports of personnel security investigations and the pre-employment screening process. Most investigations are conducted on an agency's behalf by external investigative organizations. However, some agencies conduct their own investigations under a delegated investigative authority from the Office of Personnel Management (OPM) or similar organization. Often, agencies which conduct their own security checks operate their own employment systems, also under delegated authority from OPM.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 18, item 22b (NC1-GRS-80-1 item 23b)

*Destroy in accordance with the investigating agency instruction*

\* Similar records have been approved as temporary. Personnel Security Investigation Case Files-XML copy of case files exported from JSTARS, DAA-0436-2012-0007-0001.

\* Has little or no research value. Records are administrative in nature.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. Item 170 is unchanged and supersedes GRS 18, item 22b (NC1-GRS-80-1 item 23b). Item 071 is new and provides disposition authority for the reports generated by agencies conducting investigations under a delegated authority. These reports must be retained for a sufficient amount of time to ensure reciprocity, where an investigation can be checked should an employee transfer to another agency or require his or her clearance be transferred to another organization.

**Media Neutrality:** Approved

**Item 0024 (GRS 5.6, item 180): Personnel security and access clearance records-Records of persons not issued clearances.**

**Item 0025 (GRS 5.6, item 181): Personnel security and access clearance records- Records of persons issued clearances.**

These items provide disposition authority for personnel security and access clearance case files. The new items separate unfavorably adjudicated cases from the favorable cases. This is a

significant change from the previous GRS 18, item 22a which covered case files of all persons regardless of whether a clearance was issued.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 18, item 22a (NC1-GRS-80-1, item 23a) *5 years*

\* Has little or no research value. Records are administrative in nature.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. Item 180, a new item, provides agencies the legal authority to destroy case files of persons not issued clearances within 1 year after consideration. It also provides authority to keep them longer should there be a business need. Agencies requested the addition of this item during subject matter expert meetings to address the issue the security portion of applicant case files. We are proposing a similar 1-year retention of job application packages in GRS 2.1, not yet issued. Item 181 retains the 5-year retention period established by old GRS 18, item 22a with the exception of the statement “Destroy upon notification of death” which we removed to simplify the instruction. The 5-year retention should suffice. Under item 181, agencies may keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0026 (GRS 5.6, item 190): Personnel security and access clearance status records.**

This item provides disposition authority for records used by agencies to manage the security clearance renewal process by keeping track of personnel security and access clearances.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 18, item 22c (NC1-GRS-80-1, item 23c) *Destroy with related case file*

GRS 18, item 23 (NC1-GRS-80-1, item 24) *when superseded or obsolete*

\* Has little or no research value. Records are administrative in nature. The records covered under this item are associated with non-supervisory, administrative and/or routine activities.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. This new item aggregates GRS 18, item 22c, Index to the Personnel Security Case Files, and GRS 18, item 23, Personnel Security Clearance Status File into a single authority. The retention period is unchanged from older versions of the items. While the retention is the same as GRS 4.1, item 010, Tracking and control records, item 010 cannot be used because it excludes records containing abstracts of records content or other information that can be used as an information source apart from the related records. Agencies may keep records longer if they have a business need to do so.

**Media Neutrality:** Approved

**Item 0027 (GRS 5.6, item 200): Information security violations records- Cases referred to investigative agencies.**

**Item 0028 (GRS 5.6, item 201): Information security violations records- All other cases.**

These items cover case files of alleged violations of Executive orders, laws, or agency regulations for the safeguarding of national security information. We added the term “information” to the item in order to differentiate these violations from other types.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\* Previously approved as temporary.

GRS 18, item 24a (NC1-GRS-81-8, item 1a) *5 years*

GRS 18, item 24b (N1-GRS-98-2, item 31) *2 years*

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. The retention periods of the items remain the same with the exception of a statement being added to each instruction permitting longer retention if the records are required for business use.

**Media Neutrality:** Approved

**Item 0029 (GRS 5.6, item 210): Insider threat protection administrative and operations records.**

**Item 0030 (GRS 5.6, item 220): Insider threat protection inquiry records.**

**Item 0031 (GRS 5.6, item 230): Insider threat protection data collection.**

These 3 items cover records of executive branch agencies responsible for implementing insider threat protection programs under Executive Order 13587. An insider threat is defined as a threat posed to U.S. national security by someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to any U.S. Government resource. This threat can include damage through espionage, terrorism, sabotage, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. All executive branch agencies with access to classified information are mandated to set up insider threat detection programs.

Insider threat programs are found Government-wide within security and personnel security offices. Agency insider threat programs target anomalous activities, not individuals, and are not considered investigatory in nature. Rather, agencies gather and search records to look for trends which might suggest suspicious activities. Some agencies have limited their programs to searching the records of security clearance holders and others have expanded their data collection to all persons who engage with an agency. Should an agency discover an anomaly it will report the finding to the National Insider Threat Task Force (NITFF). If responsive, the NITFF in turn will refer the matter for investigation by the appropriate investigatory agency, typically the Federal Bureau of Investigation for criminal referrals. Non-criminal agency investigations will be referred to an agency’s internal Office of Inspector General or other relevant agency office such as human resources, personnel security, or security depending on the nature of the matter.

**Proposed Disposition:** Temporary

**Appropriateness of Proposed Disposition:** Appropriate

**Appraisal Justification:**

\*Similar records have been approved as temporary. Security Violations Case Files, NC1-GRS-81-8, item 1a and N1-GRS-98-2, item 31; MSD/CI 2 Insider Threat Case Files, N1-576-12-1, item 10.

\*Captured elsewhere in permanent records. Threats of significance are reported to the NITTF. If NITTF agrees the threat or activity warrants further investigation or review it is referred to the appropriate investigatory agency, either the Federal Bureau of Investigation or internal agency Office of Inspector General (IG), based on the subject matter or nature of activity for further review and/or action. For example, if the threat was referred to Office of the Director of National Intelligence's IG, the records would be captured in the appropriate investigation reports and case files, proposed as permanent in N1-576-11-11, item IG-1a or in minor and routine case files, proposed as temporary in N1-576-11-11, item IG-1e.

\*Does not document significant actions of Federal officials.

**Adequacy of Proposed Retention Period:** Adequate from the standpoint of legal rights and accountability. Item 210 covers administrative and operations records of the insider threat protection programs. Records are kept to document routine program activities. A 7 year retention period will meet agency business needs for these records. Item 220 addresses the searches generated by the agencies and sent for referral. A 7-year retention period following the case referral was discussed during work group meetings with agency subject matter experts and thought to provide a minimum retention period sufficient to meet agency business needs.

Item 230 covers the insider threat data collection. An agency's data collection is an aggregation of records, most of which are not unique as they are copies of other records used for trend analysis. A minimum retention period of 25 years coupled with the flexibility to keep records longer was thought by agency subject matter experts to be the lowest possible minimum retention threshold for the records. As some agencies are only beginning their data collection activities, this item will require reassessment as agency insider threat protection programs mature. A couple of agencies have proposed related temporary items for case files which are pending approval, including: Security Financial Disclosure Program (PII), DAA-0537-2015-0001-0001 (25 years after separation) and Insider Threat Program Inquiry Case Files, DAA-478-2015-0003-0001(30 years after close of inquiry). Agencies may keep records longer if they have a business need to do so.

**Media Neutrality:** Approved



LAURA ADAMS McHALE

Appraiser

New GRS 5.6				Old GRS			
GRS No.	Item No.	Retention	Disposition Authority	GRS No.	Item No.	Retention	Disposition Authority
5.6	010	3 years	DAA-GRS-2016-00xx-0001	18	8	2 years	GRS 18, 1960, item 9
				18	13a	3 years	GRS 18, 1960, item 14a
				18	13b	2 years	GRS 18, 1960, item 14b
				18	21	2 years	NC1-GRS-80-1, item 22
5.6	020	3 years	DAA-GRS-2016-00xx-0002	18	16a	3 years	GRS 18, 1960, item 17
5.6	021	6 months	DAA-GRS-2016-00xx-0003	18	16b	6 months	GRS 18, 1960, item 17
5.6	030	3 months	DAA-GRS-2016-00xx-0004	18	19d	3 months	GRS 18, 1960, item 20d
5.6	040	3 months	DAA-GRS-2016-00xx-0005	18	12	3 months	GRS 18, 1960, item 13
5.6	050	3 years	DAA-GRS-2016-00xx-0006	12	8 (in part)	3 years	NC1-64-77-9, item 8 (in part)
5.6	060	3 years	DAA-GRS-2016-00xx-0007	18	15a (in part)	3 years	GRS 18, 1960, item 16a (in part)
				18	15b (in part)	1 year	GRS 18, 1960, item 16b (in part)
5.6	061	30 days	DAA-GRS-2016-00xx-0008	18	15a (in part)	3 years	GRS 18, 1960, item 16a (in part)
				18	15b (in part)	1 year	GRS 18, 1960, item 16b (in part)
5.6	070	10 years	DAA-GRS-2016-00xx-0009	New item.			
5.6	080	5 years	DAA-GRS-2016-00xx-0010	18	9 (in part)	3 years	GRS 18, 1960, item 10 (in part)
				18	10 (in part)	4 years	GRS 18, 1960, item 11 (in part)
5.6	081	3 years	DAA-GRS-2016-00xx-0011	18	9 (in part)	3 years	GRS 18, 1960, item 10 (in part)
				18	10 (in part)	4 years	GRS 18, 1960, item 11 (in part)
5.6	090	30 days	DAA-GRS-2016-00xx-0012	18	18a	1 year	GRS 18, 1960, item 19a
				18	18b	1 month	GRS 18, 1960, item 19b
				18	19a	Superseded or obsolete	GRS 18, 1960, item 20a
				18	19b	1 year	GRS 18, 1960, item 20b
				18	19c	1 year	GRS 18, 1960, item 20c
				21	11	6 months	N1-GRS-98-2, item 37
				21	18	6 months	N1-GRS-98-2, item 39
5.6	100	3 years	DAA-GRS-2016-00xx-0013	10	13	1 year	N1-GRS-04-6, item 5
				18	11	2 years	GRS 18, 1960, item 12
				18	14a	3 years	GRS 18, 1960, item 15a
				18	14b	2 years	GRS 18, 1960, item 15b
				18	14c	1 year	GRS 18, 1960, item 15c
5.6	110	5 years	DAA-GRS-2016-00xx-0014	18	17a	5 years	GRS 18, 1960, item 18
				18	20a (in part)	2 years	GRS 18, 1960, item 21a (in part)
				18	20b (in part)	1 year	GRS 18, 1960, item 21b (in part)
5.6	111	3 years	DAA-GRS-2016-00xx-0015	18	17b	2 years	GRS 18, 1960, item 18
				18	20a (in part)	2 years	GRS 18, 1960, item 21a
				18	20b (in part)	1 year	GRS 18, 1960, item 21b
5.6	120	5 years	DAA-GRS-2016-00xx-0016	11	4a (in part)	3 months	GRS 11, 1952, item 4a (in part)
				11	4b (in part)	When accounted for	GRS 11, 1952, item 4b (in part)
				21	2 (in part)	5 years	N1-GRS-98-2, item 33 (in part)
5.6	121	Expiration or confiscation	DAA-GRS-2016-00xx-0017	New item.			
5.6	130	3 months	DAA-GRS-2016-00xx-0018	11	4a (in part)	3 months	GRS 11, 1952, item 4a (in part)
				11	4b (in part)	When accounted for	GRS 11, 1952, item 4b (in part)
				21	2 (in part)	5 years	N1-GRS-98-2, item 33 (in part)
5.6	140	When accredited	DAA-GRS-2016-00xx-0019	New item.			
5.6	150	5 years	DAA-GRS-2016-00xx-0020	New item.			
5.6	160	3 years	DAA-GRS-2016-00xx-0021	New item.			
5.6	170	Per agency instruction	DAA-GRS-2016-00xx-0022	18	22b	Per agency instruction	NC1-GRS-80-1, item 23b
5.6	171	Per agreement or MOU	DAA-GRS-2016-00xx-0023	New item.			
5.6	180	1 year	DAA-GRS-2016-00xx-0024	New item.			
5.6	181	5 years	DAA-GRS-2016-00xx-0025	18	22a	5 years	NC1-GRS-80-1, item 23a
5.6	190	Superseded or obsolete	DAA-GRS-2016-00xx-0026	18	22c	With related case file	NC1-GRS-80-1, item 23c
				18	23	Superseded or obsolete	NC1-GRS-80-1, item 24
5.6	200	5 years	DAA-GRS-2016-00xx-0027	18	24a	5 years	NC1-GRS-81-8, item 1a
5.6	201	2 years	DAA-GRS-2016-00xx-0028	18	24b	2 years	N1-GRS-98-2, item 31
5.6	210	7 years	DAA-GRS-2016-00xx-0029	New item.			
5.6	220	7 years	DAA-GRS-2016-00xx-0030	New item.			
5.6	230	25 years	DAA-GRS-2016-00xx-0031	New item.			