DAA-GRS-2013-0006

This file contains three documents. The "ERA Version" of the schedule is the official version as it appears in the Electronic Records Archives. Its presentation is heavily fielded to ERA architecture. You may find the "Review Version" (the format that will appear when the approved schedule is published online) easier to read. Both versions contain the same information. The Appraisal Memorandum provides additional background explanation and includes the appraiser's justification for the retention decisions proposed in the schedule.

National Archives and Records Administration
Office of the Chief Records Officer
GRS Team
May 1, 2013

Request for Records Disposition Authority

Records Schedule Number	DAA-GRS-2013-0006
Schedule Status	Appraiser Working Version
Agency or Establishment	General Records Schedules (National Archives and Records Administration)
Record Group / Scheduling Group	General Records Schedules
Records Schedule applies to	Government-wide
Schedule Subject	Information Systems Security Records
Internal agency concurrences will be provided	No

Background Information

This schedule provides disposal authorization for certain files created and maintained in the operation and management of information technology (IT) and related services. As defined in the Clinger-Cohen Act, "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

The E-Government Act recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, titled the Federal Information Security Management Act (FISMA), emphasized the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

Item Count

Number of Total Disposition Items	Number of Permanent Disposition Items	Number of Temporary Disposition Items	Number of Withdrawn Disposition Items
8	0	8	0

GAO Approval

Outline of Records Schedule Items for DAA-GRS-2013-0006

Sequence Number	
1	Systems and Data Security Records Disposition Authority Number: DAA-GRS-2013-0006-0001
2	Computer Security Incident Handling, Reporting and Follow-up Records Disposition Authority Number: DAA-GRS-2013-0006-0002
3	System Access and Monitoring Records
3.1	Systems Not Requiring Special Accountability for Access Disposition Authority Number: DAA-GRS-2013-0006-0003
3.2	Systems Requiring Special Accountability for Access Disposition Authority Number: DAA-GRS-2013-0006-0004
4	System Backups and Tape Library Records
4.1	Incremental backup files Disposition Authority Number: DAA-GRS-2013-0006-0005
4.2	Full backup files Disposition Authority Number: DAA-GRS-2013-0006-0006
5	Backups of Master Files and Databases
5.1	File identical to records scheduled for transfer to the National Archives. Disposition Authority Number: DAA-GRS-2013-0006-0007
5.2	File identical to records authorized for destruction by a NARA-approved records schedule. Disposition Authority Number: DAA-GRS-2013-0006-0008

Records Schedule Items

Sequence Number

1 Systems and Data Security Records

Disposition Authority Number: DAA-GRS-2013-0006-0001

These are records related to maintaining the security of systems and data. Systems and Data Security records include those such as: • System Security Plans • Disaster Recovery Plans • risk analyses used in identifying IT risks and analyzing their impact • risk measurements and assessments • actions to mitigate risks • implementation of risk action plans • service test plans • test files and data

Final Disposition	Temporary
Item Status	Pending
Is this item media neutral?	Yes
Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	Yes
Do any of the records covered by this item exist as structured electronic data?	Yes
GRS or Superseded Authority Citation	N1-GRS-03-1 item 5a N1-GRS-03-1 item 5b

Disposition Instruction

Retention Period	Destroy 1 year(s) after system is superseded

Additional Information

GAO Approval	Not Required

2 Computer Security Incident Handling, Reporting and Follow-up Records

Disposition Authority Number: DAA-GRS-2013-0006-0002

A computer incident within the Federal Government as defined by NIST Special Publication 800-61 is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. This item covers records relating to attempted or actual system security breaches, including break-ins ("hacks," including virus attacks), improper staff usage, failure of security provisions or procedures, and potentially compromised information assets. It also includes agency reporting of such incidents both internally and externally. Computer Security Incident Handling, Reporting and Follow-up Records include those such as: • narrative reports • background documentation

	Final Disposition	Temporary
	Item Status	Pending
	Is this item media neutral?	Yes
	Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	Yes
	Do any of the records covered by this item exist as structured electronic data?	Yes
	GRS or Superseded Authority Citation	N1-GRS-03-1 item 7
	Disposition Instruction	
	Retention Period	Destroy 3 year(s) after all necessary follow-up actions have been completed
	Additional Information	
	GAO Approval	Not Required
3	System Access and Monitoring Records Files created as part of the user identification and authorization process to gain access to systems and monitor system usage. System Access and Monitoring records include those such as: • user profiles • log-in files • password files • audit trail files and extracts • system usage files • cost-back files used to assess charges for system use EXCLUSIONS: (1) Excludes records relating to electronic signatures. (2) Internal agency system use does not include monitoring for agency mission activities such as law enforcement.	
3.1	Systems Not Requiring Special Accountability for Access	
	Disposition Authority Number	DAA-GRS-2013-0006-0003
	Files created as part of the user identification and authorization process to gain access to systems and monitor system usage.	
	Final Disposition	Temporary
	Item Status	Pending
	Is this item media neutral?	Yes
	Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	Yes
	Do any of the records covered by this item exist as structured electronic data?	Yes

	GRS or Superseded Authority Citation	N1-GRS-95-2 item 1c
	Disposition Instruction	
	Retention Period	Destroy 1 year(s) after user account is terminated or password is altered or when no longer needed for investigative or security purposes, whichever is appropriate
	Additional Information	
	GAO Approval	Not Required
3.2	Systems Requiring Special Accountability for Access	
	Disposition Authority Number	DAA-GRS-2013-0006-0004
	Files created as part of the user identification and authorization process to gain access to systems and monitor system usage. These are systems which contain information that may be needed for audit or investigative purposes and those that contain classified records	
	Final Disposition	Temporary
	Item Status	Pending
	Is this item media neutral?	Yes
	Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	Yes
	Do any of the records covered by this item exist as structured electronic data?	Yes
	GRS or Superseded Authority Citation	N1-GRS-03-1 item 6a
	Disposition Instruction	
	Retention Period	Destroy 6 year(s) after user account is terminated or password is altered or when no longer needed for investigative or security purposes, whichever is later.
	Additional Information	
	GAO Approval	Not Required
4	System Backups and Tape Library Records Backup files maintained for potential system restoration in the event of a system failure or other unintentional loss of data.	
4.1	Incremental backup files	

	Disposition Authority Number	DAA-GRS-2013-0006-0005
	Final Disposition	Temporary
	Item Status	Pending
	Is this item media neutral?	Yes
	Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	No
	GRS or Superseded Authority Citation	N1-GRS-03-1 item 4a1
	Disposition Instruction	
	Retention Period	Destroy when superseded by a full backup, or when no longer needed for system restoration, whichever is later
	Additional Information	
	GAO Approval	Not Required
4.2	Full backup files	
	Disposition Authority Number	DAA-GRS-2013-0006-0006
	Final Disposition	Temporary
	Item Status	Pending
	Is this item media neutral?	Yes
	Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	Yes
	Do any of the records covered by this item exist as structured electronic data?	Yes
	GRS or Superseded Authority Citation	N1-GRS-03-1 item 4a2
	Disposition Instruction	
	Retention Period	Destroy when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.
	Additional Information	
	GAO Approval	Not Required

5

Backups of Master Files and Databases
Electronic copy, considered by the agency to be a Federal record, of the master copy of an electronic record or file and retained in case the master file or database is damaged or inadvertently erased.

5.1

File identical to records scheduled for transfer to the National Archives.

Disposition Authority Number	DAA-GRS-2013-0006-0007
Final Disposition	Temporary
Item Status	Pending
Is this item media neutral?	Yes
Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	Yes
Do any of the records covered by this item exist as structured electronic data?	Yes
GRS or Superseded Authority Citation	N1-GRS-95-2 item 8a

Disposition Instruction

Retention Period	Destroy immediately after the identical records have been captured in a subsequent backup file or at any time after the transfer request has been signed by the National Archives

Additional Information

GAO Approval	Not Required

5.2

File identical to records authorized for destruction by a NARA-approved records schedule.

Disposition Authority Number	DAA-GRS-2013-0006-0008
Final Disposition	Temporary
Item Status	Pending
Is this item media neutral?	Yes
Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing?	Yes
Do any of the records covered by this item exist as structured electronic data?	Yes

GRS or Superseded Authority Citation	N1-GRS-95-2 item 8b
Disposition Instruction	
Retention Period	Destroy immediately after the identical records have been deleted or replaced by a subsequent backup file
Additional Information	
GAO Approval	Not Required

Agency Certification

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal in this schedule are not now needed for the business of the agency or will not be needed after the retention periods specified.

Signatory Information

Date	Action	By	Title	Organization
04/30/2013	Certify	Margaret Hawkins	Director of Records Management Services	National Records Management Program - Records Management Services

Executive Summary

Summary

Permanent Item Numbers

Federal Register Notice

Publication Date

Copies Requested	0
Comments Received	0

NOTE: This schedule is intended to be used as an alternate review version of a Request for Records Disposition Authority submitted for approval in the Electronic Records Archive (ERA). This version contains the same information that is in ERA with one exception, it has provided hierarchical overview and item numbers. These numbers reflect the manual citation numbers that will appear in the manual version of the GRS published on NARA's website.

REQUEST FOR RECORDS DISPOSITION AUTHORITY

Records Schedule Number: DAA-GRS-2013-0006
Agency or Establishment: General Records Schedules (National Archives and Records Administration)
Records Group: General Records Schedules
Record Schedule applies to: Government-wide
Schedule Subject: Information Systems Security Records

Background Information:
This schedule provides disposal authorization for certain files created and maintained in the operation and management of information technology (IT) and related services. As defined in the Clinger-Cohen Act, "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
The E-Government Act recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, titled the Federal Information Security Management Act (FISMA), emphasized the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

1. Systems and Data Security Records

These are records related to maintaining the security of systems and data.

Systems and Data Security records include those such as:

- System Security Plans
- Disaster Recovery Plans
- risk analyses used in identifying IT risks and analyzing their impact
- risk measurements and assessments
- actions to mitigate risks
- implementation of risk action plans
- service test plans
- test files and data

Disposition: Temporary. Destroy 1 year(s) after system is superseded.
Disposition Authority: DAA-GRS-2013-0006-0001
Media Neutral: Yes.

Supersedes: N1-GRS-03-1 item 5a (GRS 24, item 5a); N1-GRS-03-1 item 5b (GRS 24, item 5b)
GAO Approval: Not Required

2. Computer Security Incident Handling, Reporting and Follow-up Records

A computer incident within the Federal Government as defined by NIST Special Publication 800-61 is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. This item covers records relating to attempted or actual system security breaches, including break-ins ("hacks," including virus attacks), improper staff usage, failure of security provisions or procedures, and potentially compromised information assets. It also includes agency reporting of such incidents both internally and externally.

Computer Security Incident Handling, Reporting and Follow-up Records include those such as:

- narrative reports
- background documentation

Disposition: Temporary. Destroy 3 year(s) after all necessary follow-up actions have been completed.
Disposition Authority: DAA-GRS-2013-0006-0002
Media Neutral: Yes.
Supersedes: N1-GRS-03-1 item 7 (GRS 24, item 7)
GAO Approval: Not Required

3. System Access and Monitoring Records

Files created as part of the user identification and authorization process to gain access to systems and monitor system usage.

System Access and Monitoring records include those such as:

- user profiles
- log-in files
- password files
- audit trail files and extracts
- system usage files
- cost-back files used to assess charges for system use

EXCLUSIONS:
(1) Excludes records relating to electronic signatures.
(2) Internal agency system use does not include monitoring for agency mission activities such as law enforcement.

a. Systems Not Requiring Special Accountability for Access
Files created as part of the user identification and authorization process to gain access to systems and monitor system usage.

Disposition: Temporary. Destroy 1 year after user account is terminated or password is altered or when no longer needed for investigative or security purposes, whichever is later.
Disposition Authority: DAA-GRS-2013-0006-0003
Media Neutral: Yes.
Supersedes: N1-GRS-95-2 item 1c (GRS 20, item 1c)
GAO Approval: Not Required

b. Systems Requiring Special Accountability for Access
Files created as part of the user identification and authorization process to gain access to systems and monitor system usage. These are systems which contain information that may be needed for audit or investigative purposes and those that contain classified records.

Disposition: Temporary. Destroy 6 years after user account is terminated or password is altered or when no longer needed for investigative or security purposes, whichever is later.
Disposition Authority: DAA-GRS-2013-0006-0004
Media Neutral: Yes.
Supersedes: N1-GRS-03-1 item 6a (GRS 24, item 6a)
GAO Approval: Not Required

4. System Backups and Tape Library Records
Backup files maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

a. Incremental backup files

Disposition: Temporary. Destroy when superseded by a full backup, or when no longer needed for system restoration, whichever is later.
Disposition Authority: DAA-GRS-2013-0006-0005
Media Neutral: Yes.
Supersedes: N1-GRS-03-1 item 4a1 (GRS 24 item 4a1)
GAO Approval: Not Required

b. Full backup files

Disposition: Temporary. Destroy when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.

Disposition Authority: DAA-GRS-2013-0006-0006
Media Neutral: Yes.
Supersedes: N1-GRS-03-1 item 4a2 (GRS 24 item 4a2)
GAO Approval: Not Required

5. Backups of Master Files and Databases

Electronic copy, considered by the agency to be a Federal record, of the master copy of an electronic record or file and retained in case the master file or database is damaged or inadvertently erased.

a. File identical to records scheduled for transfer to the National Archives.

Disposition: Temporary. Destroy immediately after the identical records have been captured in a subsequent backup file or at any time after the transfer request has been signed by the National Archives.
Disposition Authority: DAA-GRS-2013-0006-0007
Media Neutral: Yes.
Supersedes: N1-GRS-95-2 item 8a (GRS 20, item 8a)
GAO Approval: Not Required

b. File identical to records authorized for destruction by a NARA-approved records schedule.

Disposition: Temporary. Destroy immediately after the identical records have been deleted or replaced by a subsequent backup file.
Disposition Authority: DAA-GRS-2013-0006-0008
Media Neutral: Yes.
Supersedes: N1-GRS-95-2 item 8b and GRS 20, item 8b
GAO Approval: Not Required

NATIONAL ARCHIVES and
RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

Date: April 29, 2013
Appraiser: Laura Adams McHale, ACNR
Agency: General Records Schedules (GRS)
Subject: DAA-GRS-2013-0006

AMR 4/29/13

INTRODUCTION

Schedule Overview
Information Systems Security Records

Additional Background Information
This schedule provides disposal authorization for records pertaining to the protection of federal information and information systems from unauthorized access, use, disclosure, disruptions, modification, or destruction. It also covers the creation and implementation of security policies, procedures and controls. This is a new sub-function within the Technology Management portion of the GRS.

There are no new items on this schedule. NARA formerly included these items as part of GRS 24, Information Technology Operations and Management Records and GRS 20, Electronic Records.

NARA developed this schedule with assistance from the following agencies: Department of Energy/Sandia Labs, Department of Health and Human Services, National Aeronautics and Space Administration, Department of Justice, Department of Labor, Federal Deposit Insurance Corporation, National Park Service, Social Security Administration, and the US Environmental Protection Agency. NARA further refined the schedule using comments received from the following volunteer agencies: Department of Housing and Urban Development, Office of Inspector General, Federal Housing Finance Agency, US Government Accountability Office, the National Reconnaissance Office and the Nuclear Regulatory Commission.

Overall Recommendation

I recommend approval of the attached schedule.

APPRAISAL

Item 0001: Systems and Data Security
These are records about testing, planning, and assessing risk to the security of systems and data. This item combines the current GRS 24, items 5a & 5b: Files Related to Maintaining the Security of Systems and Data because they are similar functions with the same retention.

Proposed Disposition: Temporary
Appropriateness of Proposed Disposition: Appropriate
Appraisal Justification:

* Previously approved as temporary. Files Related to Maintaining the Security of Systems and Data- System Security Plans and Disaster Recovery Plans, N1-GRS-03-1 item 5a. Files Related to Maintaining the Security of Systems and Data- Documents identifying IT risks and analyzing their impact, risk measurements and assessments, actions to mitigate risks, implementation of risk action plan, service test plans, test files and data, N1-GRS-03-1 item 5b.

Adequacy of Proposed Retention Period: Adequate from the standpoint of legal rights and accountability. This item merges 2 previously approved GRS items that had the same 1 year retention because there is no longer a separate Office of Management and Budget requirement to develop risk analysis reports. Consultation with agencies indicated a 1 year retention would meet present business needs.
Media Neutrality: Approved

Item 0002: Computer Security Incident Handling, Reporting and Follow-up Records
These records typically consist of narrative reports and background documentation relating to individual events or issues. These records would include references to unauthorized intrusions, web site defacement, misuse of system resources, and other incidents noted by the United States Computer Emergency Readiness Team (US-CERT).
Proposed Disposition: Temporary
Appropriateness of Proposed Disposition: Appropriate
Appraisal Justification:

*Previously approved as temporary. Computer Security Incident Handling, Reporting and Follow-up Records, N1-GRS-03-1 item 7.

Adequacy of Proposed Retention Period: Adequate from the standpoint of legal rights and accountability. There has been no change to the retention from the current GRS 24, item 7. Retaining records for 3 years after all follow-up actions, including judicial procedures, have been completed ensures the availability of active case records and provides an adequate amount of time after a case is closed for any necessary follow-up action. Any significant incidents (e.g., a major system failure or compromise of critical government data) would be documented in program records, such as those in the office of the Inspector General, which must be scheduled separately.
Media Neutrality: Approved

Item 0003: System Access and Monitoring Records-Systems Not Requiring Special Accountability
The records covered under this item address routine system access and routine system usage monitoring. The existing GRS 24, item 6b: User Identification, Profiles, Authorizations, and Password Files is just a pointer to GRS 20, item 1c: Files/Records Relating to the Creation, Use, and Maintenance of Computer Systems, Applications, or Electronic Records—Records created to monitor system usage, which is the item being superseded.
Proposed Disposition: Temporary
Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

* Previously approved as temporary. Files/Records Relating to the Creation, Use, and Maintenance of Computer Systems, Applications, or Electronic Records- Electronic files and hard copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files, system usage files, and cost-back files used to assess charges for system use, N1-GRS-95-2, item 1c.

Adequacy of Proposed Retention Period: Adequate from the standpoint of legal rights and accountability. The previous retention was to delete when no longer needed. Consultation with agencies indicated a 1 year retention would meet present business needs.
Media Neutrality: Approved

Item 0004: System Access and Monitoring Records-Systems Requiring Special Accountability for Access

The records covered under this item address system access and system usage monitoring for systems requiring special accountability, e.g., those containing information that may be needed for audit or investigative purposes and those that contain classified records.
Proposed Disposition: Temporary
Appropriateness of Proposed Disposition: Appropriate
Appraisal Justification:

* Previously approved as temporary. User Identification, Profiles, Authorizations, and Password Files, EXCLUDING records relating to electronic signatures- Systems requiring special accountability, e.g., those containing information that may be needed for audit or investigative purposes and those that contain classified records, N1-GRS-03-1, item 6a.

Adequacy of Proposed Retention Period: Adequate from the standpoint of legal rights and accountability. There has been no change to the retention from the current GRS 24, item 6 a.
Media Neutrality: Approved

Item 0005: System Backups and Tape Library Records- Incremental backup files
Item 0006: System Backups and Tape Library Records- Full backup files

Records are incremental and full backups of systems.
Proposed Disposition: Temporary
Appropriateness of Proposed Disposition: Appropriate
Appraisal Justification:

* Previously approved as temporary. System Backups and Tape Library Records- Incremental backup tapes, N1-GRS-03-1, item 4a1. System Backups and Tape Library Records- Full backup tapes, N1-GRS-03-1, item 4a2.

Adequacy of Proposed Retention Period: Adequate from the standpoint of legal rights and accountability. There are no changes to the proposed retention for either of these items.
Media Neutrality: Approved

Item 0007: Backups of Master Files and Databases- File identical to records scheduled for transfer to the National Archives.

Item 0008: Backups of Master Files and Databases-File identical to records authorized for destruction by a NARA-approved records schedule.

Records are essentially copies of files either transferred to NARA or disposable.

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

* Previously approved as temporary. Backups of Files- File identical to records scheduled for transfer to the National Archives, N1-GRS-95-2 item 8a. Backups of Files- File identical to records authorized for disposal in a NARA-approved records schedule, N1-GRS-95-2 item 8b.

Adequacy of Proposed Retention Period: Adequate from the standpoint of legal rights and accountability. There are no changes to the proposed retention for either of these items. Wording has been added to clarify records may be deleted once the National Archives signs the transfer request.

Media Neutrality: Approved

LAURA ADAMS McHALE
Appraiser