GENERAL RECORDS SCHEDULE (GRS) 3.2: Information Systems Security Records

This schedule covers records created and maintained by Federal agencies related to protecting the security of information technology systems and data, and responding to computer security incidents. This schedule does not apply to system data or content.

Item	Records Title/Description	Disposition Instruction	Disposition Authority
010	**Systems and data security records.** These are records related to maintaining the security of information technology (IT) systems and data. Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific systems for which they were written. This series also includes analysis of security policies, processes, and guidelines, as well as system risk management and vulnerability analyses. Includes records such as: • System Security Plans • Disaster Recovery Plans • Continuity of Operations Plans • published computer technical manuals and guides • examples and references used to produce guidelines covering security issues related to specific systems and equipment • records on disaster exercises and resulting evaluations • network vulnerability assessments • risk surveys • service test plans • test files and data	**Temporary.** Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.	DAA-GRS-2013-0006-0001
020	**Computer security incident handling, reporting and follow-up records.** A computer incident within the Federal Government as defined by NIST Special Publication 800-61, Computer Security Incident Handling Guide, Revision 2, (August 2012) 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. Includes records such as: • reporting forms	**Temporary.** Destroy 3 year(s) after all necessary follow-up actions have been completed~~, but longer retention is authorized if required for business use~~.	DAA-GRS-2013-0006-0002

Item	Records Title/Description		Disposition Instruction	Disposition Authority
	• reporting tools • narrative reports • background documentation **Note:** Any significant incidents (e.g., a major system failure or compromise of critical government data) must be documented in program records, such as those in the office of the Inspector General, which must be scheduled separately by submitting an SF 115 to NARA.		**Utilize GRS 5.6, item 200 for investigations related to national security or privacy.**	
030	**System access records.** These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records 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 **Exclusion 1.** Excludes records relating to electronic signatures. **Exclusion 2.** Does not include monitoring for agency mission activities such as law enforcement.	**Systems not requiring special accountability for access.** These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users.	**Temporary.** ~~Destroy when business use ceases.~~ **DOE Business Use: Destroy 1 year after system access terminated.**	DAA-GRS-2013-0006-0003
031		**Systems requiring special accountability for access.** These are user identification records associated with systems which are highly sensitive and potentially vulnerable.	**Temporary.** Destroy 6 years after password is altered or user account is terminated~~, but longer retention is authorized if required for business use~~.	DAA-GRS-2013-0006-0004
035	**Cybersecurity logging records.**	**Full packet capture data.**	**Temporary.** Destroy when 72 hours old. ~~Longer retention is~~	DAA-GRS-2022-0005-0001

Item	Records Title/Description		Disposition Instruction	Disposition Authority
	For additional information about these records, see OMB Memo M-21-31. **Note:** The requirements in OMB Memo M-21-31 do not apply to national security systems. Agencies may use this GRS for national security systems or submit an agency-specific schedule.	Packet capture (PCAP) results from the interception and copying of a data packet that is crossing or moving over a specific computer network. **Legal citation:** OMB Memo M-21-31 **Not media neutral.** Applies to electronic records only.	~~authorized for business use.~~	
036		**Cybersecurity event logs.** Logs required by OMB Memo M-21-31 to capture data used in the detection, investigation, and remediation of cyber threats. **Legal citation:** OMB Memo M-21-31 **Not media neutral.** Applies to electronic records only.	**Temporary.** Destroy when 30 months old. ~~Longer retention is authorized for business use.~~	DAA-GRS-2022-0005-0002
040	**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.	**Incremental backup files.**	**Temporary.** Destroy when superseded by a full backup, or when no longer needed for system restoration, whichever is later.	DAA-GRS-2013-0006-0005
041		**Full backup files.**	**Temporary.** Destroy when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.	DAA-GRS-2013-0006-0006

Item	Records Title/Description			Disposition Instruction	Disposition Authority
050	**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.	**File identical to permanent records scheduled for transfer to the National Archives.**		**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~~, but longer retention is authorized if required for business use~~.	DAA-GRS-2013-0006-0007
051		**File identical to temporary records authorized for destruction by a NARA-approved records schedule.**		**Temporary.** Destroy immediately after the identical records have been deleted or replaced by a subsequent backup file~~, but longer retention is authorized if required for business use~~.	DAA-GRS-2013-0006-0008
060	**PKI administrative records.** Records are PKI-unique administrative records that establish or support authentication by tying the user to a valid electronic credential and other administrative non-PKI records that are retained to attest to the reliability of the PKI transaction process. Included are policies and procedures planning records; stand-up configuration and validation records; operation records; audit and monitor records; and termination, consolidation, or reorganizing records. Policies and procedures planning records relate to defining and establishing PKI systems. Records relate to such activities as determining that a PKI should be established; creating		**FBCA CAs.**	**Temporary.** ~~Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer~~	N1-GRS-07-3, item 13a1

Item	Records Title/Description		Disposition Instruction	Disposition Authority
	project implementation plans; creating the certificate policy (CP), certification practice statement (CPS), and other key operating documents; developing procedures in accordance with the CP and CPS; conducting risk analyses; developing records management policies (including migration strategies); and selecting the entity that will serve as registration authority (RA). Stand-up configuration and validation records relate to installing and validating both the Certification Authority (CA) and Registration Authority (RA), obtaining final approval or rejection from the agency's oversight or authorizing body, creating and generating a CA signature key, testing security procedures for the CA and RA, validating certification revocation procedures, and establishing back-up and storage for the PKI system. Operation records relate to the certification application; certificate issuance and key generation (including key pair generation and private key loading and storage of private keys and components of private keys); certificate acceptance, validation, revocation, suspension, replacement, and renewal; creating and maintaining an event log; and installing and validating software updates. Audit and monitor records relate to conducting periodic internal and external reviews of auditable events specified in the Federal Bridge Certification Authority (FBCA) X.509 Certificate Policy and other Entity CA policies, monitoring compliance with security requirements specified in the CPS and other operating procedures, investigating internal fraud or misconduct, and conducting internal and external audits of software and systems security. Termination, consolidation, or reorganization records relate to terminating, consolidating, or reorganizing a PKI; notifying subscribers of decisions, transferring inactive keys and revocation certificate lists to storage repositories, transferring consenting subscribers' and certificates and related materials to a new Certificate Authority, destroying sensitive records involving privacy (in accordance with an authorized records schedule), and shutting down and disposing of RA hardware and CA software. **Note:** Select PKI administrative records serve as transaction records that must be retained as part of the trust documentation set with transaction-specific records. Agencies must determine which PKI administrative records are embedded with transaction-specific records as transaction records. These administrative records may vary from transaction-to-transaction.		~~needed for business, whichever is later.~~ **DOE Business Use: Destroy when 7 years and 6 months old.**	
061		**Other (non-FBCA *et. al*.) CAs.**	**Temporary.** ~~Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.~~ **DOE Business Use: Destroy when 7 years and 6 months old.**	N1-GRS-07-3 , item 13a2

Item	Records Title/Description	Disposition Instruction	Disposition Authority
062	**PKI transaction-specific records.** Records relate to transaction-specific records that are generated for each transaction using PKI digital signature technology. Records are embedded or referenced within the transaction stream and may be appended to the transaction content or information record. Along with PKI administrative and other administrative records, transaction-specific records are part of the PKI trust documentation set that establish or support the trustworthiness of a transaction. They may vary from transaction-to- transaction and agency-to-agency. When retained to support the authentication of an electronic transaction content record (information record), PKI digital signature transaction records are program records. **Note:** Extreme care must be taken when applying the GRS-PKI to transaction records. Destruction of the transaction-specific and administrative records embedded in the transaction stream prior to the authorized retention of the information record that they access/protect will render the PKI incapable of performing what it is designed to do-protect and provide access to the information record. Due to the relative newness of PKI technology, both from an implementation and a litigation perspective, it is recommended that agencies identify all PKI transaction records (including PKI select administrative records embedded in the transaction stream and transaction-specific records) to be retained as part of the trust documentation for the records the PKI is designed to protect and or access and link the retention of the transaction records with that of the information record it protects/accesses. Transaction records must be retained as trust documentation set records together with the content/information record.	**Temporary.** ~~Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the appropriate CA and after the information record the PKI is designed to protect and/or access is destroyed according to an authorized schedule, or in the case of permanent records, when the record is transferred to NARA legal custody. Longer retention is authorized if the agency determines that transaction-specific PKI records are needed for a longer period~~. **DOE Business Use: Destroy when 7 years and 6 months old.**	N1-GRS-07-3, item 13b