SERIES 1600 – GENERAL IT MANAGEMENT

SERIES TITLE: GENERAL INFORMATION TECHNOLOGY MANAGEMENT RECORDS

SERIES DESCRIPTION: Records described in this series relate to the creation and management of electronic records, by computer operators, programmers, analysts, systems administrators, information technology (IT) offices (operation and management), and all personnel with access to a computer, to include contractors. Disposition authority is provided for certain master files, including some tables that are components of database management systems, and certain files created from master files for specific purposes. In addition, this series covers certain disposable electronic records produced by end users in office automation applications. This series provides authority to apply disposition instructions found elsewhere in this records schedule to electronic files and dispose of hard copy documents when converted to electronic media, if specified requirements have been met (See AI 15 and 36 CFR 1234 for additional guidance).

NOTE: This series does not apply to master files and other related records produced by electronic information systems (EIS) that HAVE NOT been evaluated by WHS, Records, Privacy and Declassification Division; contact RDD to determine if scheduling of such records is required.

SERIES APPLIES TO THE FOLLOWING ORGANIZATIONS: File Numbers within the 1600 Series may be used by any directorate, division, branch, task force, field office or component under the purview of the OSD Records Administrator.

RECORDS CATEGORY: 1601
CATEGORY TITLE: General
CATEGORY DESCRIPTION: General or overview file numbers pertaining to electronic records.

FILE NUMBER: 1601-01
FILE TITLE: System Development Records
FILE DESCRIPTION: These records related to development of Information Technology (IT) systems and software applications through their initial stages up until hand-off to production which includes planning, requirements analysis, design, verification and testing, procurement, and installation. Records include case files containing documentation of planning, decision making, designing, programming, testing, evaluation, and problem solving. Includes records such as:

- Project plans
- Feasibility studies
- Cost analyses
- Requirements documents
- Compliance documents including:
  - Privacy Threshold Analyses (PTAs)
  - Privacy Impact Assessments (PIAs)
  - Security Plan
  - Information Protection Plan
- Change control records
- Project Schedule
- Plan of Action and Milestones (POA&M)

- Configuration Management Plan
- Resource Management Plan
- Risk Assessment/Mitigation Plan
- Security Plan
- Disaster Recovery Plan
- Test/Acceptance Plan
- Quality Control Plan
- Deployment Guide
- User Guide
- Training Guide

Exclusion: This item does not apply to system data or content.
NOTE: For certain technical documentation (e.g., data dictionaries, file specifications, code books, record layouts, etc.) related to the detailed, as-built design or maintenance of an electronic system containing permanent records, use the GRS item Documentation Necessary for Preservation of Permanent Electronic Records.
DISPOSITION: Temporary. Cut off after system is superseded by a new iteration, or is terminated, defunded, or when no longer needed for administrative, legal, audit, or other operational purposes. Destroy 5 years after cutoff.
AUTHORITY: GRS 3.1, item 011 (DAA-GRS- 2013-0005- 0007)
PRIVACY ACT: Not Applicable
FORMER FILE NUMBER: 1601-01.1

FILE NUMBER: 1601-01.1 – Consolidated into 1601-01, 1606-02 or 1606-11, as applicable
FILE NUMBER: 1601-01.2 – Consolidated into 1606-02
FILE NUMBER: 1601-01.3 – Consolidated into 1601-02

FILE NUMBER: 1601-02
FILE TITLE: System Access Records - Systems not requiring Special Accountability for Access
FILE DESCRIPTION: User identification and authorization 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. These records are created as part of the user identification and authorization process to gain access to systems. Records are also 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.
DISPOSITION: Temporary. Cut off and destroy when business use ceases. **NOTE:** See 1601-18 for System Access Records Requiring Special Accountability
AUTHORITY: GRS 3.2, item 030 (DAA-GRS-2013-0006-0003)
PRIVACY ACT: Not Applicable
FORMER FILE NUMBER(s): 1601-01.3, 1606-06.2

FILE NUMBER: 1601-02.1 – RESCINDED (per GRS Transmittal 23)
FILE NUMBER: 1601-02.2 – RESCINDED (per GRS Transmittal 23)
FILE NUMBER: 1601-02.3 – RESCINDED (per GRS Transmittal 23)
FILE NUMBER: 1601-02.4 – Consolidated into 103-14
FILE NUMBER: 1601-02.5 – Consolidated into 1606-02
FILE NUMBER: 1601-02.6 – Consolidated into 1606-02
FILE NUMBER: 1601-02.7 – Consolidated into 1606-02

FILE NUMBER: 1601-03
FILE TITLE: Backups of Master Files and Databases – Files Identical to Permanent Records
FILE DESCRIPTION: 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 where the file is identical to permanent records scheduled for transfer to NARA.
DISPOSITION: Temporary. Cut off and 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 NARA.
AUTHORITY: GRS 3.2, item 050 (DAA-GRS-2013-0006-0007)
PRIVACY ACT: K890.14-DoD

FILE NUMBER: 1601-03.1 – RESCINDED (per GRS Transmittal 23)
FILE NUMBER: 1601-03.2 – RESCINDED (per GRS Transmittal 23)
FILE NUMBER: 1601-03.3 – RESCINDED (per GRS Transmittal 23)
FILE NUMBER: 1601-03.4 – RESCINDED (per GRS Transmittal 23)
FILE NUMBER: 1601-03.5 – RESCINDED (per GRS Transmittal 23)
FILE NUMBER: 1601-04 – RESCINDED (per GRS Transmittal 23)
FILE NUMBER: 1601-05 – Consolidated into 103-14
FILE NUMBER: 1601-06 – Consolidated into 103-14
FILE NUMBER: 1601-07 – Consolidated into 103-14
FILE NUMBER: 1601-08 – Consolidated into 103-14

FILE NUMBER: 1601-09
FILE TITLE: Backups of Master Files and Databases – Identical to Temporary Records
FILE DESCRIPTION: 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 where the file is identical to temporary records authorized for disposal in a NARA-approved records schedule.
DISPOSITION: Temporary. Cut off and destroy immediately after the identical temporary records have been deleted, or when replaced by a subsequent backup file.
AUTHORITY: GRS 3.2, item 051 (DAA-GRS-2013-0006-0008)
PRIVACY ACT: Not Applicable

FILE NUMBER: 1601-10 – Consolidated into 203-05

FILE NUMBER: 1601-11
FILE TITLE: Special Purpose Computer Programs and Applications

FILE DESCRIPTION: Computer software programs or applications that are developed by the agency or under its direction solely to use or maintain a master file or database authorized for disposal by this records disposition schedule or by a NARA-approved records schedule.
Exclusion 1: This item does not include software or applications necessary to use or maintain any unscheduled master file or database or any master file or database scheduled for transfer to the National Archives.
Exclusion 2: This item does not cover commercial, off-the-shelf (COTS) programs or applications, unless the agency has modified such programs or applications considerably to perform a mission-related function.
NOTE: Computer software needs to be kept as long as needed to ensure access to, and use of, the electronic records in the system throughout the authorized retention period to comply with 36 CFR Sections 1236.10, 1236.12, 1236.14, and 1236.20.
DISPOSITION: Temporary. Cut off and destroy when related master file or database has been deleted.
AUTHORITY: GRS 3.1, item 012 (DAA-GRS-2013-0005-0008)
PRIVACY ACT: Not Applicable

FILE NUMBER: 1601-12.1 – Moved to 1601-12
FILE NUMBER: 1601-12.2 – Moved to 1601-13

FILE NUMBER: 1601-12
FILE TITLE: Data Administration and Documentation - Temporary Systems
FILE DESCRIPTION: Data administration records and documentation relating to electronic records that are scheduled as temporary in the GRS or this schedule or any types of data administration records not listed as permanent in File Number 1601-12.2. Includes

- Data/database dictionary records
- Data system specifications
- File specifications
- Code books
- Record layouts
- Metadata
- User guides
- Output specifications.

Also includes the following records for all electronic records whether scheduled as temporary or permanent:

- Software operating manuals
- Data standards
- Table and dependency descriptions
- Taxonomies
- Schemas
- Registries
- Source code
- Physical data model
- Logical data model

DISPOSITION: Temporary. Cut off after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system. Destroy 5 years after cutoff.
AUTHORITY: GRS 3.1, item 051 (DAA-GRS-2013-0005-0003)
PRIVACY ACT: Not Applicable
FORMER FILE NUMBER: 1601-12.1

FILE NUMBER: 1601-13
FILE TITLE: Data Administration and Documentation - Permanent Systems
FILE DESCRIPTION: Data administration records and documentation relating to electronic records scheduled as permanent in the GRS or this schedule must be transferred to NARA to allow for continued access to the records. Includes

- Data/database dictionary records
- Data systems specifications
- File specifications
- Code books
- Record layouts
- Metadata
- User guides
- Output specifications.

NOTE 1: Per NARA practice, documentation for permanent electronic records must be transferred with the related records using the disposition authority for the related electronic records rather than the GRS disposition authority.
NOTE 2: Agencies may retain a copy of documentation related to permanent electronic records. This copy may be destroyed at any time after the transfer request has been signed by NARA.
DISPOSITION: Permanent. Cut off and transfer to NARA with the permanent electronic records to which the documentation relates.
AUTHORITY: GRS 3.1, item 050 (DAA-GRS-2013-0005-0002)
PRIVACY ACT: Not Applicable
FORMER FILE NUMBER: 1601-12.2

FILE NUMBER: 1601-13.1 – Consolidated into 103-14
FILE NUMBER: 1601-13.2 – Consolidated into 103-14
FILE NUMBER: 1601-13.3 – Consolidated into 1606-02
FILE NUMBER: 1601-14 – Consolidated into 103-14
FILE NUMBER: 1601-15 – Consolidated into 103-14
FILE NUMBER: 1601-16 – Consolidated into 103-14

FILE NUMBER: 1601-17
FILE TITLE: Non-recordkeeping copies of electronic records
FILE DESCRIPTION: Non-recordkeeping copies of electronic records maintained in email systems, computer hard drives or networks, web servers, or other location after the recordkeeping copy has been copied to a recordkeeping system or otherwise preserved. This includes:

- Documents such as letters, memoranda, reports, handbooks, directives, manuals, briefings or presentations created on office applications, including Portable Document Format (PDF) or its equivalent

- Senders' and recipients' versions of electronic mail messages that meet the definition of Federal records and any related attachments after they have been copied to an recordkeeping system or otherwise preserved
- Electronic spreadsheets
- Digital video or audio files
- Digital maps or architectural drawings
- Copies of the above electronic records maintained on websites or web servers, but EXCLUDING web pages themselves

NOTE 1: Not all copies are non-record. Copies are non-record if they are kept only for convenience of reference. If copies are used in the course of agency business to make decisions or take action they are a federal record. The records described here are records, but not recordkeeping copies of those records.
NOTE 2: For electronic mail records the recordkeeping system must capture the names of sender and recipients and date (transmission data for recordkeeping purposes) and any receipt data when required along with the message text. Sender/recipient information should be individual account information, not the name of a distribution list.
DISPOSITION: Temporary. Cut off and destroy immediately after copying to a recordkeeping system or otherwise preserving.
AUTHORITY: GRS 5.1, Item 020 (DAA-GRS-2016-0016-0002)
PRIVACY ACT: Not Applicable
FORMER FILE NUMBER(s): 1602, 1603, 1604-01, 1604-02, 1703-01

FILE NUMBER: 1601-18
FILE TITLE: System Access Records - Systems requiring Special Accountability for Access
FILE DESCRIPTION: User identification records associated with systems which are highly sensitive and potentially vulnerable. These records are created as part of the user identification and authorization process to gain access to such systems. Records are also 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.
DISPOSITION: Temporary. Cut off when password is altered of user account is terminated. Destroy 6 years after cutoff.
NOTE: See 1601-02 for System Access Records Not Requiring Special Accountability
AUTHORITY: GRS 3.2, item 031 (DAA-GRS-2013-0006-0004)
PRIVACY ACT: Not Applicable

RECORDS CATEGORY: 1602 – RESERVED

FILE NUMBER: 1602 – Consolidated into 1601-17

RECORDS CATEGORY: 1603 – RESERVED

FILE NUMBER: 1603 – Consolidated into 1601-17

RECORDS CATEGORY: 1604 – RESERVED

FILE NUMBER: 1604-01 – Consolidated into 1601-17
FILE NUMBER: 1604-02 – Consolidated into 1601-17

RECORDS CATEGORY: 1605 – RESERVED

FILE NUMBER: 1605-01 – Consolidated into 101-01.1
FILE NUMBER: 1605-02 – Consolidated into 101-01.1

RECORDS CATEGORY: 1606
CATEGORY TITLE: Information Technology Operations and Management Records
CATEGORY DESCRIPTION: Provides disposal authorization for certain files created and maintained in the operation and management of information technology (IT) and related services. IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. **NOTE:** System data or information content must be scheduled separately to NARA; contact RDD to coordinate in such a situation.

FILE NUMBER: 1606-01
FILE TITLE: Information Technology Oversight and Compliance Records
FILE DESCRIPTION: Information technology (IT) oversight and compliance records relate to compliance with IT policies, directives, and plans. Records are typically found in offices with agency-wide or bureau-wide responsibility for managing IT operations. Includes such records as:

- Recurring and special reports
- Responses to findings and recommendations
- Reports of follow-up activities
- Statistical performance data
- Metrics
- Inventory of web activity
- Web use statistics
- Comments/feedback from web site or application users
- Internal and external reporting for compliance requirements relating to the Privacy Act, and electronic and Information technology accessibility under Section 508 of the Rehabilitation Act
- System availability reports
- Target IT architecture reports
- Systems development lifecycle handbooks
- Computer network assessments and follow-up documentation
- Vulnerability assessment reports
- Assessment and authorization of equipment
- Independent Verification and Validation (IV&V) reports
- Contractor evaluation reports

- Quality assurance reviews and reports
- Market analyses and performance surveys
- Benefit-cost analyses
- Make vs. buy analysis
- Reports on implementation of plans
- Compliance reviews
- Data measuring or estimating impact and compliance

NOTE: Copies of security plans are scheduled under the GRS for Information Security Records. There may be copies interfiled within this series.
DISPOSITION: Temporary. Cut off annually. Destroy 5 years after cutoff or 1 year after responsible office determines that there are no unresolved issues, whichever is longer.
AUTHORITY: GRS 3.1, item 040 (DAA-GRS-2013-0005-0010)
PRIVACY ACT: Not Applicable
FORMER FILE NUMBER(s): 1606-01.1, 1606-01.2

FILE NUMBER: 1606-01.1 – Consolidated into 1606-01
FILE NUMBER: 1606-01.2 – Consolidated into 1606-01

FILE NUMBER: 1606-02
FILE TITLE: Information Technology (IT) Operations and Maintenance Records
FILE DESCRIPTION: IT operations and maintenance records relate to the activities associated with the operation and maintenance of the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Includes the activities associated with IT equipment, IT systems and storage media, IT system performance testing, asset and configuration management, change management, and maintenance on network infrastructure.

- Files identifying IT facilities and sites
- Files concerning implementation of IT facility and site management
- Equipment support services provided to specific sites:
    - Reviews
    - Site visit reports
    - Trouble reports
    - Equipment service histories
    - Reports of follow-up actions
    - Related correspondence
- Inventories of IT assets, network circuits, and building or circuitry diagrams
- Equipment control systems such as databases of barcodes affixed to IT physical assets, and tracking of [approved] personally-owned devices
- Requests for service
- Work orders
- Service histories
- Workload schedules
- Run reports
- Schedules of maintenance and support activities
- Problem reports and related decision documents relating to the software infrastructure of the network or system
- Reports on operations
    - Measures of benchmarks

    - Performance indicators
    - Critical success factors
    - Error and exception reporting
    - Self-assessments
    - Performance monitoring
    - Management reports
- Website administration
    - Frames
    - Templates
    - Style sheets
    - Site maps
    - Codes that determine site architecture
    - Change requests
    - Site posting logs
    - Clearance records
    - Requests for correction of incorrect links or content posted
    - Requests for removal of duplicate information
    - User logs
    - Search engine logs
    - Audit logs
- Records to allocate charges and track payment for software and services

NOTE 1: If any maintenance activities have a major impact on a system or lead to a significant change, those records should be maintained as part of the Configuration and Change Management Records.
NOTE 2: Records needed to support contracts should be in procurement files, which are scheduled under the GRS for General Financial Management Records.
DISPOSITION: Temporary. Cut off after the project/activity/transaction is completed or superseded. Destroy 5 years after cutoff.
AUTHORITY: GRS 3.1, item 020 (DAA-GRS-2013-0005-0004)
PRIVACY ACT: Not Applicable
FORMER FILE NUMBER(s): 1601-01.1, 1601-01.2, 1601-02.5, 1601-02.6, 1601-02.7, 1601-13.3, 1606-02.1, 1606-03.1, 1606-03.2.2, 1606-08.1, 1606-08.2, 1606-08.3, 1606-09.1, 1606-09.2, 1606-09.3

FILE NUMBER: 1606-03
FILE TITLE: Configuration and Change Management Records
FILE DESCRIPTION: Records created and retained for asset management, performance and capacity management, system management, configuration and change management, and planning, follow-up, and impact assessment of operational networks and systems. Includes records such as:

- Data and detailed reports on implementation of systems, applications and modification
- Application sizing, resource and demand management records
- Documents identifying, requesting and analyzing possible changes, authorizing changes, and documenting implementation of changes
- Documents of software distribution (including COTS software license management files) and release or version management files

NOTE 1: If any maintenance activities have a major impact on a system or lead to a significant change, those records should be maintained as part of the Configuration and Change Management Records.

NOTE 2: Documentation for permanent electronic records should be transferred with the related records using the disposition authority for the related electronic records rather than this GRS disposition authority.
NOTE 3: Agencies may retain a copy of documentation related to permanent electronic records. This copy may be destroyed at any time after the transfer request has been signed by the National Archives.
DISPOSITION: Temporary. Cut off after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes. Destroy 5 years after cutoff.
AUTHORITY: GRS 3.1, item 030 (DAA-GRS-2013-0005-0005
PRIVACY ACT: Not Applicable
FORMER FILE NUMBER: 1606-03.2.1

FILE NUMBER: 1606-03.1 – Consolidated into 1606-02
FILE NUMBER: 1606-03.2.1 – Moved to 1606-03
FILE NUMBER: 1606-03.2.2 – Consolidated into 1606-02

FILE NUMBER: 1606-04.1
FILE TITLE: System Backups and Tape Library Records - Incremental Backup Files
FILE DESCRIPTION: Incremental backup files maintained for potential system restoration in the event of a system failure or other unintentional loss of data. **NOTE:** See FN 1601-05 for backups of master files and databases.
DISPOSITION: Temporary. Cut off and destroy when superseded by a full backup, or when no longer needed for system restoration, whichever is later.
AUTHORITY: GRS 3.2, item 040 (DAA-GRS-2013-0006-0005)
PRIVACY ACT: Not Applicable

FILE NUMBER: 1606-04.2
FILE TITLE: System Backups and Tape Library Records – Full Backup Files
FILE DESCRIPTION: Full backup files maintained for potential system restoration in the event of a system failure or other unintentional loss of data. **NOTE:** See FN 1601-05 for backups of master files and databases.
DISPOSITION: Temporary. Cut off and destroy when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.
AUTHORITY: GRS 3.2, item 041 (DAA-GRS-2013-0006-0006)
PRIVACY ACT: Not Applicable

FILE NUMBER: 1606-05
FILE TITLE: Systems and Data Security Records
FILE DESCRIPTION: 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. Also includes analysis of security policies, processes, and guidelines, as well as system risk management and vulnerability analyses. Includes such records 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

DISPOSITION: Temporary. Cut off 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. Destroy 1 year after cutoff.
AUTHORITY: GRS 3.2, item 010 (DAA-GRS-2013-0006-0001)
PRIVACY ACT: Not Applicable
FORMER FILE NUMBER(s): 1606-05.1, 1606-05.2

FILE NUMBER: 1606-05.1 – Consolidate into 1606-05
FILE NUMBER: 1606-05.2 – Consolidate into 1606-05

FILE NUMBER: 1606-06
FILE TITLE: System Access Records for Systems Requiring Special Accountability for Access
FILE DESCRIPTION: User identification records associated with systems which are highly sensitive and potentially vulnerable. 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.
NOTE: See 1601-02 for System Access Records Not Requiring Special Accountability
DISPOSITION: Temporary. Cut off after password is altered or user account is terminated. Destroy 6 years after cutoff.
AUTHORITY: GRS 3.2, item 031 (DAA-GRS-2013-0006-0004)
PRIVACY ACT: K890.14-DoD
FORMER FILE NUMBER: 1606-06.1

FILE NUMBER: 1606-06.1 – Moved to 1606-06
FILE NUMBER: 1606-06.2 – Consolidated into 1601-02

FILE NUMBER: 1606-07
FILE TITLE: Computer Security Incident Handling, Reporting and Follow-Up Records
FILE DESCRIPTION: 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. 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. Includes records such as:

- Reporting forms
- 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 and be scheduled separately with NARA; contact RDD to coordinate in such a situation.
DISPOSITION: Temporary. Cut off after all necessary follow-up actions have been completed. Destroy 3 years after cutoff.
AUTHORITY: GRS 3.2, item 020 DAA-GRS-2013-0006-0002)
PRIVACY ACT: Not Applicable

FILE NUMBER: 1606-08
FILE TITLE: Technology Management Administrative Records
FILE DESCRIPTION: Records on day-to-day, routine information technology management (excluding record of the Chief Information Officer, which are located in Records Category 1105). Records include:

- Correspondence
- Subject files, including briefings, reports, presentations, and studies that do not relate to high-level decision-making
- Data calls
- Operational and managerial guidance to organizational segments of the Agency

DISPOSITION: Temporary. Cut off annually. Destroy 5 years after cutoff.
AUTHORITY: GRS 3.1, item 001 (DAA-GRS-2016-0013-0002)
PRIVACY ACT: Not Applicable

FILE NUMBER: 1606-08.1 – Consolidated into 1606-02
FILE NUMBER: 1606-08.2 – Consolidated into 1606-02
FILE NUMBER: 1606-08.3 – Consolidated into 1606-02
FILE NUMBER: 1606-09.1 – Consolidated into 1606-02
FILE NUMBER: 1606-09.2 – Consolidated into 1606-02
FILE NUMBER: 1606-09.3 – Consolidated into 1606-02

FILE NUMBER: 1606-10
FILE TITLE: Technical and Administrative Help Desk Operational Records
FILE DESCRIPTION: Records related to technical and administrative help desk operations. Includes:

- Records of incoming requests (and responses) made by phone, email, web portal, etc.
- Trouble tickets and tracking logs
- Quick Guides and “Frequently Asked Questions” (FAQs)
- Evaluations and feedback about help desk services
- Analysis and reports generated from customer management data
- Customer/client feedback and satisfaction surveys, including survey instruments, data, background materials, and reports

DISPOSITION: Temporary. Cut off after record is resolved or when no longer needed, whichever is appropriate. Destroy 1 year after cutoff.
AUTHORITY: GRS 5.8, item 010 (DAA-GRS-2017-0001-0001)

PRIVACY ACT: Not Applicable
FORMER FILE NUMBER(s): 1606-10.1, 1606-10.2

FILE NUMBER: 1606-10.1 – Consolidated into 1606-10
FILE NUMBER: 1606-10.2 – Consolidated into 1606-10

FILE NUMBER: 1606-11
FILE TITLE: Infrastructure Project Records
FILE DESCRIPTION: Information Technology (IT) Infrastructure, systems, and service project records that document the basic systems and services used to supply the agency and its staff access to computers and data telecommunications. Includes requirements for and implementation of functions such as

- Maintaining network servers, desktop computers, and other hardware
- Installing and upgrading network operating systems and shared applications
- Providing data telecommunications; and infrastructure development and maintenance such as acceptance/authorization of infrastructure components, analysis of component options, feasibility, costs and benefits, and work associated with implementation, modification, and troubleshooting.

Includes such records as:

- Installation and testing records
- Installation reviews and briefings
- Quality assurance and security review
- Requirements specifications
- Technology refresh plans
- Operational support plans
- Test plans
- Models, diagrams, schematics, and technical documentation

Exclusion: Records relating to specific systems that support or document mission goals are not covered by this item and must be scheduled individually by the agency by submission of a records schedule to NARA.
NOTE: Records concerning the development of each information technology (IT) system and software application are covered under the item for System Development Records (File Number 1601-01.1).
DISPOSITION: Temporary. Cut off after project is terminated. Destroy 5 years after cutoff.
AUTHORITY: GRS 3.1, item 010 (DAA-GRS-2013-0005-0006
PRIVACY ACT: Not Applicable
FORMER FILE NUMBER(s): 1601-01.1, 1606-11.1, 1606-11.2, 1606-11.3

FILE NUMBER: 1606-11.1 – Consolidated into 1606-11
FILE NUMBER: 1606-11.2 – Consolidated into 1606-11
FILE NUMBER: 1606-11.3 – Consolidated into 1606-11

FILE NUMBER: 1606-12
FILE TITLE: Public Key Infrastructure (PKI) Administrative Records – Federal Bridge Certification Authority (FBCA) Certification Authority
FILE DESCRIPTION: 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 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.
DISPOSITION: Temporary. Cutoff annually. Destroy 7 years and 6 months, 10 years and 6 months, or 20 years and 6 months after cutoff, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.
AUTHORITY: GRS 3.2, item 060 (N1-GRS-07-3, item 13a(1))
PRIVACY ACT: Not Applicable

FILE NUMBER: 1606-13
FILE TITLE: Public Key Infrastructure (PKI) Administrative Records – Non-Federal Bridge Certification Authority (Non-FBCA) Certification Authority
FILE DESCRIPTION: 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 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.
DISPOSITION: Temporary. Cut off annually. Destroy 7 years 6 months to 20 years 6 months after cutoff, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.
AUTHORITY: GRS 3.2, item 061 (N1-GRS-07-3, item 13a(2))
PRIVACY ACT: Not Applicable

FILE NUMBER: 1606-14
FILE TITLE: Public Key Infrastructure (PKI) Transaction-Specific Records
FILE DESCRIPTION: 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.
DISPOSITION: Temporary. Cut off annually. Destroy 7 years 6 months to 20 years 6 months after cutoff, 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.
AUTHORITY: GRS 3.2, item 062 (N1-GRS-07-3, item 13b)
PRIVACY ACT: Not Applicable

FILE NUMBER: 1606-15
FILE TITLE: Computer Matching Program Notices and Agreements
FILE DESCRIPTION: Agency copy of notices of intent to share data in systems of records with other Federal, state, or local government agencies via computer matching programs, and related records documenting publication of notice in the Federal Register per the Privacy Act of 1974 [5 U.S.C. 552a(e)(12)], as amended. Also agreements between agencies, commonly referred to as Computer Matching Agreements, prepared in accordance with Office of Management and Budget Final Guidance. Includes documentation of Data Integrity Board (DIB) review and approval of matching programs and agreements, and significant background material documenting formulation of notices and agreements.

DISPOSITION: Temporary. Cut off and destroy upon supersession by a revised notice of agreement OR two years after matching program ceases operation.
AUTHORITY: GRS 4.2, item 170 (DAA-GRS-2016-0003-0005)
PRIVACY ACT: Not Applicable

FILE NUMBER: 1606-16
FILE TITLE: Cybersecurity Full Packet Capture Data Logging Records
FILE DESCRIPTION: Packet capture (PCAP) results from the interception and copying of a data packet that is crossing or moving over a specific computer network.
DISPOSITION: Temporary. Cut off and destroy when 72 hours old.
AUTHORITY: GRS 3.2, item 035 (DAA-GRS-2022-0005-0001)
PRIVACY ACT: Not Applicable
NOTE 1: Legal Citation is OMB M-21-31.
NOTE 2: Records are not media neutral (applies to electronic PCAP records only).

FILE NUMBER: 1606-17
FILE TITLE: Cybersecurity Event Logs
FILE DESCRIPTION: Logs required by OMB Memo M-21-31 to capture data used in the detection, investigation, and remediation of cyber threats.
DISPOSITION: Temporary. Cut off monthly. Destroy 30 months after cutoff.
AUTHORITY: GRS 3.2, item 036 (DAA-GRS-2022-0005-0002)
PRIVACY ACT: Not Applicable
NOTE 1: Legal Citation is OMB M-21-31.
NOTE 2: Records are not media neutral (applies to electronic PCAP records only).

RECORDS CATEGORY: 1607 – Moved to Records Category 1105

FILE NUMBER: 1607-01 – Consolidated to 1105-01
FILE NUMBER: 1607-02 – Moved to 1105-02
FILE NUMBER: 1607-03 – Consolidated into 1105-01
FILE NUMBER: 1607-04 – Moved to 1105-03
FILE NUMBER: 1607-05 – Consolidated into 1105-01
FILE NUMBER: 1607-06 – RESCINDED per GRS Transmittal 27