NATIONAL ARCHIVES

OFFICE *of the* CHIEF RECORDS OFFICER

The General Records Schedules

Transmittal 33

National Archives and Records Administration
January 2023

Table of Contents

Other schedules were issued under previous Transmittals.
You can access all GRS schedules in this table or this PDF.

TO: Heads of federal agencies

1. What does this document do?

GRS Transmittal 33 announces changes to the General Records Schedules (GRS) made since NARA published GRS Transmittal 32 in March 2022. The GRS provide mandatory disposition instructions for records common to several or all Federal agencies.

Transmittal 33 includes alterations to three previously published schedules. As with the past few transmittals, this transmittal publishes only those schedules which have changed since they were last published in a transmittal. Other schedules *not* published in this transmittal remain current and authoritative. You can find all schedules (in Word and PDF formats), a master crosswalk, FAQs for all schedules, and FAQs about the whole GRS at http://www.archives.gov/records-mgmt/grs.html.

2. What changes does this transmittal make to the GRS?

GRS Transmittal 33 publishes updates to:

GRS 2.3 Employee Relations Records (see question 3 below)

GRS 3.2 Information Systems Security Records (see question 4 below)

GRS 6.1 Email and Other Electronic Messages Managed Under a Capstone Approach (see question 5 below)

3. What changes did we make to GRS 2.3, Employee Relations Records?

We updated items 010 and 020 to incorporate records related to religious accommodations. Previously, these items only covered records related to reasonable accommodations.

4. What changes did we make to GRS 3.2, Information Systems Security Records?

We added items 035 and 036 for cybersecurity logging records to support record retention requirements established in OMB Memo M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents.

5. What changes did we make to GRS 6.1, Email and Other Electronic Messages Managed Under a Capstone Approach?

This update expands the scope of GRS 6.1 beyond email to certain electronic messages, as reflected in the title change: "Email and Other Electronic Messages Managed under a Capstone Approach."

Agencies will now have the option of applying the GRS 6.1 Capstone approach to:

- electronic messages affiliated with email system chat or messaging functions, where the messages are managed independently from the email;
- messages from messaging services provided on mobile devices; and
- messages from messaging services on third-party applications.

Agencies still must submit NARA Form NA-1005, Verification for the Use of GRS 6.1, Email and Other Electronic Messages Managed Under a Capstone Approach, for approval to use GRS 6.1.

6. How do agencies cite GRS items?

When citing the legal disposition authority for records covered by the GRS on NARA documents, either when transferring records to Federal Records Centers for storage, to NARA for accessioning, or when requesting GRS deviations on record schedules, use the "DAA" number in the "Disposition Authority" column of the table. For example, "DAA-GRS-2017-0007-0008" rather than "GRS 2.2, item 070." A GRS Disposition Authority Look-Up Table is available on our website at https://www.archives.gov/records-mgmt/grs.html.

7. Do agencies have to take any action to implement these GRS changes?

If your agency chooses to use the Capstone approach to managing email and other electronic messages (GRS 6.1), your agency must first submit the form NA-1005, *Verification for the Use of GRS 6.1,* for NARA review and approval. An agency may not implement GRS 6.1 until NARA approves the form. Your agency may already have an approved form NA-1005; agencies are, however, required to resubmit form NA-1005 every four years per NARA Bulletin 2022-02, *Resubmission of Capstone Forms*. Forms are to be submitted to GRS_Team@nara.gov.

NARA regulations (36 CFR 1226.12(a)) require agencies to disseminate GRS changes within six months of receipt.

Per 36 CFR 1227.12(a)(1), you must follow GRS dispositions that state they must be followed without exception.

Per 36 CFR 1227.12(a)(3), if you have an existing schedule that differs from a new GRS item that does *not* require being followed without exception, and you wish to continue using your agency-specific authority rather than the GRS authority, you must notify NARA within 120 days of the date of this transmittal. Please send these notifications to GRS_Team@nara.gov.

If you do not have an already existing agency-specific authority but wish to apply a retention period that differs from that specified in the GRS, you must submit a records schedule to NARA for approval via the Electronic Records Archives.

8. How can an agency get copies of the new GRS?

You can download the complete current GRS, in PDF format, from NARA's web site at http://www.archives.gov/records-mgmt/grs.html.

9. Whom should an agency contact for further information?

Please contact GRS_Team@nara.gov with any questions related to this transmittal.

DEBRA STEIDEL WALL
Acting Archivist of the United States

GENERAL RECORDS SCHEDULE 2.3: Employee Relations Records

This schedule covers records documenting activities related to managing relationships between the agency, its employees, and its unions and bargaining units. Additional copies of these records, when held by supervisors or managers in program offices, are supervisory files covered under GRS 2.2, item 080.

Agencies must offer any records created prior to January 1, 1921, to the National Archives and Records Administration (NARA) before applying disposition instructions in this schedule.

Item	Records Description	Disposition Instruction	Disposition Authority
010	**Employee relations programs' administrative records.** Records documenting routine activities related to programs such as reasonable or religious accommodation, displaced employees, telework/alternative worksite opportunities, anti-harassment, Alternative Dispute Resolution (ADR), Equal Employment Opportunity (EEO), and other avenues for settling disputes. Includes: ● program-related correspondence ● copies of statutes, regulations, directives, and instructions ● timetables and guidelines for processing case files and appealing decisions ● planning records ● meeting minutes ● program evaluations and reports to senior management ● statistical records tracking program participation and participants ● records tracking programs' compliance with relevant Executive Orders and other requirements ● records arranging for outside mediator and facilitator involvement in case settlements **Exclusions:** 1. Records specific to individual cases (covered by items 020 to 111 in this schedule). 2. Reports to external oversight agencies (covered by GRS 5.7, item 050). 3. Records created by offices responsible for monitoring employee relations programs government-wide (must be scheduled individually by responsible offices).	**Temporary**. Destroy when 3 years old, but longer retention is authorized if required for business use.	DAA-GRS-2022-0001-0001
020	**Reasonable or religious accommodation case files**. Individual employee files created, received, and maintained by EEO reasonable accommodation, diversity/disability programs, employee relations coordinators, supervisors, administrators, or Human Resource specialists containing records of requests for religious accommodation, reasonable	**Temporary**. Destroy 3 years after employee separation from the agency or all appeals are	DAA-GRS-2022-0001-0002

Item	Records Description	Disposition Instruction	Disposition Authority
	accommodation and/or assistive technology devices and services that have been requested for or by an employee. Includes: ● request, approvals and denials ● notice of procedures for informal dispute resolution or appeal processes ● forms, correspondence, records of oral conversations ● policy guidance documents ● medical records ● supporting notes and documentation	concluded, whichever is later, but longer retention is authorized if required for business use.	
030	**Dislocated worker program case files**. Includes applications, registrations, supporting documentation.	**Temporary.** Destroy 1 year after employee eligibility for program expires, but longer retention is authorized if required for business use.	DAA-GRS-2018-0002-0003
040	**Telework/alternate worksite program case files**. Includes: • agency/employee agreements • records such as questionnaires relating to the safety of the worksite • records documenting worksite safety and equipment; hardware, and software installation and use; and offsite use of secure, classified information or data subject to the Privacy Act or agencies' Personally Identifiable Information policies	**Temporary.** Destroy when superseded or obsolete or 1 year after end of employee's participation in program, whichever is sooner, but longer retention is authorized if required for business use.	DAA-GRS-2018-0002-0004
050	**Harassment complaint case files**. Records of complaints regarding unwelcome workplace conduct, filed in accordance with agency policies and procedures. Includes: • complaint, correspondence, notes, forms, and supporting material • records of investigation, statements of witnesses • determination as to whether harassment occurred • documentation of preventive or corrective measures	**Temporary.** Destroy 7 years after close of case, but longer retention is authorized if required for business use.	DAA-GRS-2018-0002-0005

Item	Records Description		Disposition Instruction	Disposition Authority
	Note: If a harassment complaint is settled via the EEO, ADR, or grievance process, its records are scheduled under the item specific to that process.			
060	**Administrative grievance, disciplinary, performance-based, and adverse action case files.** • Records of grievances filed by covered entities (for instance, employees who are not members of a bargaining unit). Includes: o statement of grievance, supporting documentation, and evidence o statements of witnesses, records of interviews and hearings o examiner's findings, recommendations, decisions • Records of disciplinary and performance-based actions against employees. Includes: o performance appraisal, performance improvement plan, and supporting documents o recommended action, employee's reply o records of hearings and decisions o records of appeals • Records of adverse actions (suspension, removal, reduction in grade, reduction in pay, or furlough) against employees. Includes: o proposed adverse action, employee's reply o statements of witnesses o records of hearings and decisions o letters of reprimand o records of appeals **Note 1**: Letter of reprimand filed in an employee's Official Personnel File is scheduled by GRS 2.2, item 041. **Note 2**: Per OPM, each agency must select one fixed retention period, between 4 and 7 years, for all administrative grievance, adverse action, and performance-based action case files. Agencies may not use different retention periods for individual cases.		**Temporary.** Destroy no sooner than 4 years but no later than 7 years (see Note 2) after case is closed or final settlement on appeal, as appropriate.	DAA-GRS-2018-0002-0006
070	**Alternative Dispute Resolution (ADR) case files.** Includes: • agreements to use ADR • records of intake and process	**Informal process.** Records not associated with another employee dispute, complaint or grievance process.	**Temporary**. Destroy 3 years after case is closed, but longer disposition is authorized if required for business use.	DAA-GRS-2018-0002-0007

Item	Records Description		Disposition Instruction	Disposition Authority
071	• records of settlement or discontinuance of case • parties' written evaluations of the process	**Formal process**. Records generated in response to a referral from another dispute, grievance or complaint process, such as EEO complaints or grievances.	**Temporary.** Destroy 7 years after case is closed, but longer retention is authorized if required for business use.	DAA-GRS-2018-0002-0008
080	**Merit Systems Protection Board (MSPB) case files.** Civil Service Reform Act appeal case files involving actions appealable to MSPB per 5 CFR 1201.3. May include: • petitions for appeal, agencies' responses to petitions • hearing notices, transcripts, testimony, briefs, and exhibits • MSPB initial decisions • petitions for review, responses of opposing party to petition • orders granting or denying intervention • MSPB final opinions, orders, and decisions **Exclusion**: Corresponding case files at MSPB (must be scheduled by MSPB).		**Temporary.** Destroy 3 years after final resolution of case, but longer retention is authorized if required for business use.	DAA-GRS-2018-0002-0009
090	**Labor arbitration (negotiated grievance procedure) case records.** Records of workplace disputes processed under negotiated grievance procedures and settled by either agreement or binding arbitration.		**Temporary.** Destroy 3 years after close of case, but longer retention is authorized if required for business use.	DAA-GRS-2018-0002-0010
100	**Federal Labor Relations Authority (FLRA) case files.** Records of cases filed under provisions of the Federal Labor Relations Act concerning representation, unfair labor practices, negotiability, and review of arbitration awards. May include: • records of representation proceedings o petitions, notice of petitions, cross-petitions, motions o records documenting adequate showing of interest o challenges to the status of a labor organization o records of meetings, hearings, and prehearing conferences o statements of witnesses o dismissals of petitions		**Temporary.** Destroy 3 years after final resolution of case, but longer retention is authorized if required for business use.	DAA-GRS-2018-0002-0011

Item	Records Description		Disposition Instruction	Disposition Authority
	o decisions, orders • records of unfair labor practices proceedings o charges/allegations of unfair labor practices, amendments, and supporting evidence o records of charges/allegations investigation, including subpoenas o complaints by FLRA Regional Director o motions, responses, stipulations o records of hearings o records of decisions and settlements • records of negotiability proceedings o petitions for review o records of post-petition conferences o agencies' statements of position, unions' responses, and agencies' counter-responses o records of post-petition conferences o decisions, orders • records of review of arbitration awards o exceptions to arbitrators' award rendered pursuant to arbitrations o oppositions to exceptions o determination of grounds for review o decisions, orders **Exclusion**: Corresponding case files at FLRA (must be scheduled by FLRA).			
110	**EEO discrimination complaint case files**. Includes: • intake sheet • summary report • notes • supporting documentation • correspondence	**Informal process.** Records of cases that do not result in an EEO complaint, and cases resulting in a complaint but resolved prior to the formal process stage.	**Temporary**. Destroy 3 years after resolution of case, but longer retention is authorized if required for business use**.**	DAA-GRS-2018-0002-0012
111		**Formal process**. Records at originating agency generated in response to formal complaints resolved within the agency, by the Equal Employment Opportunity Commission, or by a U.S. Court. Includes records gathered in the preliminary informal process, complaints, exhibits, withdrawal notices, copies of decisions, and records of hearings and meetings.	**Temporary.** Destroy 7 years after resolution of case, but longer retention is authorized if required for business use.	DAA-GRS-2018-0002-0013

Item	Records Description	Disposition Instruction	Disposition Authority
	Exclusion: Corresponding case files at EEOC (must be scheduled by EEOC).		
120	**Records documenting contractor compliance with EEO regulations.** Reviews, background documents, and correspondence relating to contractor employment practices.	**Temporary.** Destroy when 7 years old, but longer retention is authorized if required for business use.	DAA-GRS-2018-0002-0014
130	**Labor management relations agreement negotiation records.** Records relating to negotiations with labor unions. Includes: • negotiation agreements • requests to bargain • bargaining session records/notes • correspondence, memoranda, forms • reports • other records relating to the negotiated agreements and general relationship between management, employee unions and other groups	**Temporary.** Destroy 5 years after expiration of agreement or final resolution of case, as appropriate, but longer retention is authorized if required for business use.	DAA-GRS-2018-0002-0015

GENERAL RECORDS SCHEDULE 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 • reporting tools	**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
	• 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.			
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.	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.** 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	**Full packet capture data.** 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	**Temporary.** Destroy when 72 hours old. Longer retention is authorized for business use.	DAA-GRS-2022-0005-0001

Item	Records Title/Description		Disposition Instruction	Disposition Authority
	use this GRS for national security systems or submit an agency-specific schedule.	**Not media neutral.** Applies to electronic records only.		
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
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	DAA-GRS-2013-0006-0007

Item	Records Title/Description		Disposition Instruction	Disposition Authority
			National Archives, but longer retention is authorized if required for business use.	
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 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	**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 needed for business, whichever is later.	N1-GRS-07-3, item 13a1
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.	N1-GRS-07-3 , item 13a2

Item	Records Title/Description	Disposition Instruction	Disposition Authority
	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.		
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	**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	N1-GRS-07-3, item 13b

Item	Records Title/Description	Disposition Instruction	Disposition Authority
	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.	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.	

GENERAL RECORDS SCHEDULE 6.1:
Email and Other Electronic Messages Managed under a Capstone Approach

This schedule applies *only* to federal agencies that implement a Capstone approach as described in this GRS. When implementing this GRS, agencies should consult the FAQs about GRS 6.1, Email and Other Electronic Messages Managed under a Capstone Approach. Agencies are reminded that this GRS should not be implemented in isolation and should be supplemented with agency-wide policies and training. Agencies must also incorporate this GRS into agency records management implementation tools, such as manuals and file plans. Agencies adopting a Capstone approach should consult other resources related to email and electronic message management, specifically the Capstone approach available on NARA's email management page.

Agencies must not implement this GRS until obtaining approval of NARA form 1005 (NA-1005), *Verification for Implementing GRS 6.1*. Agencies are required to obtain approval of a resubmitted NA-1005 at least every four years. Additional information, including a link to the form, may be found in the FAQs and in the instructions accompanying the form.

GRS Scope

This GRS provides disposition authority for email records and certain types of electronic messages. Agencies using this GRS must apply it to email records, but may choose to also apply it to the other allowable types of electronic messages outlined below; this must be documented on the NA-1005. Agencies wishing to schedule electronic messages outside the scope of this GRS may submit an agency-specific schedule proposing a different scope.

Email

This GRS applies to all email, regardless of how the email messages are managed or what email technology is used. Email, in the context of this GRS, also includes any associated attachments. This GRS may apply to records affiliated with other commonly available functions of email programs such as calendars/appointments and tasks.

Other Types of Electronic Messages

The GRS does not cover all types of electronic messages. Agencies may choose to use this GRS for instant messages, text messages, and chat messages that serve a similar purpose as email to facilitate communication and information sharing. This includes:

- messages affiliated with email system chat or messaging functions, and where the messages are managed independently from the email;
- messages from messaging services provided on mobile devices; and
- messages from messaging services on third-party applications.

Exclusions to all items below:

- messages affiliated with social media accounts/social media direct messaging services;
- messages affiliated with messaging services provided on video conferencing applications and services;
- voice mail (or similarly recorded) messages;
- messages affiliated with collaboration platforms; and
- messages from messaging systems that are ancillary to the purpose of a larger system (for example, a chat function built into a procurement system).

These records still require NARA-approved disposition authority but are not covered under this GRS. See the GRS 6.1 FAQ for specific examples of the inclusions and exclusions.

Additional Scope

Each agency is responsible for determining the scope of implementation when using Capstone, including, 1) whether implementation is to include only email, or to also include other types of electronic messages; 2) The range of implementation in an organization (agency-wide, specific office, etc.); and 3) the range of implementation regarding email and/or other types of electronic messaging technology and system platforms. Brief information on the scope of an agency's Capstone implementation is also required on the NA-1005.

Agencies are also responsible for defining (and documenting through policy) the official recordkeeping version of email and/or other types of electronic messages to be managed under a Capstone approach, especially when records are captured or retained in multiple locations (e.g., an email archive vs. the live system). Agencies will need to determine the appropriate disposition for other versions of email and other types of records, whether disposable under GRS 5.1, item 020, or as non-record.

Agencies are expected to apply documented selection criteria to cull the records of Capstone officials (permanent accounts) to the greatest extent possible before transfer to NARA. Culling refers to the removal – or otherwise excluding from capture – of nonrecord, personal, or transitory messages and attachments. Culling typically includes the removal of spam, message blasts received (such as agency-wide communications), and personal materials (such as emails or messages to family members not related to agency business). Culling may be manual, automated, or a hybrid of both. Agencies may develop their own policies and procedures for the culling of temporary accounts.

Applying this GRS

When applying this GRS in part, agencies must ensure that all other records are covered by another NARA-approved disposition authority. Agencies NOT managing any of their email or other types of electronic messages under the Capstone approach are still responsible for managing these records by applying NARA-approved records schedules.

If an agency is implementing a Capstone disposition approach different from what is provided in this GRS, the agency must submit a records schedule. For

example, an agency may want to narrow the list of required positions in item 010, use shorter retention lengths for temporary records, or extend the time frame for transfer of permanent records. Agencies who wish to use Capstone for a broader range of electronic messages, specifically those excluded from this GRS, may also submit an agency-specific schedule.

Item	Records Description	Disposition Instruction	Disposition Authority
010	**Email and other electronic messages of Capstone officials.** Capstone Officials are senior officials designated by account or position level. This may be by email addresses, whether the addresses are based on an individual's name, title, a group, or a specific program function, and/or by phone number or other identifier for other types of electronic messages. Capstone officials include all those listed on an approved NARA form 1005 (NA-1005), *Verification for Implementing GRS 6.1*, and *must* include, when applicable: 1. The head of the agency, such as Secretary, Commissioner, Administrator, Chairman or equivalent; 2. Principal assistants to the head of the agency (second tier of management), such as Under Secretaries, Assistant Secretaries, Assistant Commissioners, and/or their equivalents; this includes officers of the Armed Forces serving in comparable position(s); 3. Deputies of all positions in categories 1 and 2, and/or their equivalent(s); 4. Staff assistants to those in categories 1 and 2, such as special assistants, confidential assistants, military assistants, and/or aides; 5. Principal management positions, such as Chief Operating Officer, Chief Information Officer, Chief Knowledge Officer, Chief Technology Officer, and Chief Financial Officer, and/or their equivalent(s); 6. Directors of significant program offices, and/or their equivalent(s); 7. Principal regional officials, such as Regional Administrators, and/or their equivalent(s); 8. Roles or positions that routinely provide advice and oversight to the agency, including those positions in categories 1 through 3 and 5 through 7, including: General Counsels, Chiefs of Staff, Inspectors General, etc.; 9. Roles and positions not represented above and filled by Presidential Appointment with Senate Confirmation (PAS positions); and 10. Additional roles and positions that predominantly create permanent records related to mission critical functions or policy decisions and/or are of historical significance. This item covers emails and/or other types of electronic messages of officials captured during their tenure as a	**Permanent.** Cutoff and transfer in accordance with the agency's approved NA-1005, *Verification for Implementing GRS 6.1.* This will be between 15 and 30 years, or after declassification review (when applicable), whichever is later.	DAA-GRS-2022-0006-0001

	Capstone official only. Therefore, records created prior to their designation as a Capstone official (e.g., prior to their promotion/rotation into a Capstone position) are excluded and should be disposed of with other NARA-approved disposition authorities, including - but not limited to - items 011 and 012 of this schedule. This also includes those officials in an acting capacity for any of the above positions longer than 60 days. Agencies may also include individual emails and/or other types of electronic messages from otherwise temporary accounts appropriate for permanent disposition in this category. This item *must* include all existing legacy email and/or other types of electronic messages that correlate to the roles and positions described above. If a Capstone official has more than one agency-administered account, this item applies to all accounts. If a Capstone official has an email account managed by other staff (such as personal assistants, confidential assistants, military assistants, or administrative assistants), this item applies to those accounts. This item applies to all email and/or other types of messages regardless of the address names and/or phone number(s) used by the Capstone official for agency business, such as nicknames or office title names. Email to or from personal or non-official email and/or other messaging accounts in which official agency business is conducted is also included – a complete copy of these records must be copied or forwarded to an official electronic messaging account of the officer or employee not later than 20 days after the original creation or transmission of the record. Please consult the NA-1005 for more information on which positions are included within each category. Not media neutral; applies to records managed in an electronic format only. **Exclusions:** see exclusions under the GRS Scope section above. **Notes:** 1. Cabinet level agencies implementing a Capstone approach that includes their components/operatives must apply the above definition to each component individually. In these cases, each component/operative is considered a separate agency in terms of the above definition of Capstone Officials. A component/operative of a cabinet level agency can implement a Capstone approach independent of their department but must also conform to the entirety of this definition. 2. Smaller agencies, micro-agencies or Commissions implementing a Capstone approach may find that some of their Capstone positions fall into several of the categories above and/or that they do not have applicable roles or positions for all categories.		

011	**Email and other types of electronic messages of Non-Capstone officials.** Email and/or other types of electronic messages of all other officials, staff, and contractors not included in item 010. **Note**: Agencies *only* using item 011 and/or item 012 of this GRS may not dispose of any records of officials in item 010, Email and other electronic messages of Capstone Officials, of this GRS without authority from NARA in the form of another GRS or agency-specific schedule. Submission and approval of NA-1005 is still required in these instances to document those being exempted from Capstone. Agencies have discretion to designate individual email messages and/or other types of electronic messages, with their attachments as permanent, or as longer-term temporary records that should be cross-filed elsewhere pursuant to agency policies and business needs.	**All others except those in item 012.** Includes positions and records not covered by items 010 or 012 of this schedule. This item applies to the majority of email and other messaging accounts/users within an agency adopting a Capstone approach. Not media neutral; applies to records managed in an electronic format only. **Exclusions:** see exclusions under the GRS Scope section above.	**Temporary.** Delete when 7 years old, but longer retention is authorized if required for business use.	DAA-GRS-2022-0006-0002
012		**Support and/or administrative positions.** Includes non-supervisory positions carrying out routine and/or administrative duties. These duties comprise general office or program support activities and frequently facilitate the work of federal agencies and their programs. This includes, but is not limited to, roles and positions that: process routine transactions; provide customer service; involve mechanical crafts, or unskilled, semi-skilled, or skilled manual labor; respond to general requests for information; involve routine clerical work; and/or primarily receive nonrecord and/or duplicative email. Not media neutral; applies to records managed in an electronic format only. **Exclusions:** see exclusions under the GRS Scope section above.	**Temporary.** Delete when 3 years old, but longer retention is authorized if required for business use.	DAA-GRS-2022-0006-0003