GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2160.2B CHGE 4
October 20, 2021

GSA ORDER

SUBJECT: GSA Electronic Messaging and Related Services

1. Purpose. This Order updates GSA's directive on electronic messaging due to the move from a server-based messaging system to cloud-based email and collaboration tools and additional federal requirements for managing electronic mail records. This directive addresses security, appropriate use, and recordkeeping of the GSA Enterprise Messaging Services in a cloud-based environment.

2. Cancellation. This Order cancels and supersedes CIO 2160.2B CHGE 3, dated December 31, 2020.

3. Applicability. This Order applies to all authorized users who are granted access to the GSA enterprise messaging services and to all communications sent or received via the GSA enterprise messaging services.

4. Directive. All authorized users must comply with Federal laws and regulations relative to the GSA enterprise messaging services use, which are listed in Appendix A, References. The misuse of the GSA enterprise messaging services by authorized users can severely hamper the Agency's ability to conduct business and accomplish its mission. It is essential that users learn how to use electronic mail and collaborative tools efficiently, effectively, and courteously, practicing good security, records management, and using email in a responsible, professional, and lawful manner. Additionally, users have an obligation to be aware of computer security and privacy concerns and to guard against computer viruses. The Agency reserves the right to limit authorized users' electronic messaging access following evidence that shows prohibited or inappropriate use of the system or such use that creates an appearance of impropriety in the public view. Prohibited use is that which is forbidden by, or fails to comply with Federal laws, regulations or GSA directives.

5. Reporting Violations. All suspected violations of Federal laws and regulations relative to the GSA enterprise messaging services use; such as, security or privacy breaches, violations of Agency policy, malicious or otherwise prohibited use, shall be reported to the Information System Security Officer (ISSO) and/or Information System Security Manager (ISSM). ISSOs/ISSMs must report security incidents to the GSA Senior Agency Information Security Officer (SAISO) in accordance with CIO Procedural Guide 01-02, “Security Incident Handling.” The SAISO will determine which security incidents

should be reported to the United States Computer Emergency Readiness Team (US-CERT). The SAISO also will report incidents to the GSA Office of Inspector General (OIG) in accordance with CIO Procedural Guide 01-02. All incidents involving Personally Identifiable Information must be reported to the SAISO within one hour of discovering the incident. There should be no distinction between suspected and confirmed breaches. Anyone needing assistance in determining whether a violation has occurred may contact their local ISSO/ISSM for assistance. For ISSO, ISSM, and SAISO points of contact go to https://insite.gsa.gov/topics/information-technology/security-and-privacy/it-security/it-security-contacts-for-fisma.

6. Email Accounts and Files.

a. Email Account. An account is established between an authorized user and the GSA enterprise messaging services for the purpose of creating, sending, and receiving electronic mail messages. Email accounts are accessed using your GSA Active Directory Credentials.

(1) GSA provides annual security training for authorized users to take at the initiation of their account and to be taken annually thereafter. Any authorized user of the GSA enterprise messaging services who fails to complete the annual GSA security training will have their email account disabled. Accounts will be reinstated upon verification of the completion of the annual security training.

(2) System administrators, responsible for continued operation, maintenance, availability and accessibility of assigned system(s), will monitor all email accounts for indication of inactivity. Any email account that has not been accessed in a 90-day period will be suspended.

b. Email and Related Functionality.

(1) An Active Directory Account is required to access an email account and related functionality within a limited storage space capacity. An individual email account consists of an Inbox, Drafts, Spam, Sent, Trash, and other user-created folders for use in the creation, sending, receiving, and organization of electronic mail messages, attachments, user-saved instant messages, and digital voicemail messages received through the Voice over Internet Protocol (VoIP) telephone integration. Additional features of the GSA enterprise messaging services include calendaring, instant messaging, and collaboration tools for sharing documents, spreadsheets, presentations, and drawings.

(2) A single archive repository stores all inbound and outbound email messages and their attachments sent or received through the gsa.gov domain for e-discovery purposes for a period of time consistent with Section 4(b), "Email records retention" of GSA Order, OAS 1828.1, Email Records Management Policy. The archive repository will also be used for indefinite storage of litigation hold information.

(3) All messages and their associated attachments sent and received will be

scanned for viruses.

(4) Messages larger than 25 megabytes (MB) will not be sent or received.

7. Electronic Message Control.

a. Message Privacy. GSA provides electronic messaging services to authorized users, at GSA's expense, for their official business use for GSA or other Government business. All electronic communications sent or received are owned by the Federal Government. Occasional personal use of the electronic services that involves minimal expense to the Government, does not interfere with Government business, and otherwise conforms to GSA's personal use policy is authorized. However, authorized users have no expectation of privacy with regard to electronic messages, official or personal, sent through the Government-provided electronic messaging services, and the Agency may access, for a legitimate Governmental purpose, any message sent over its electronic services.

b. Monitoring.

(1) Obtaining access to GSA resources constitutes acknowledgment that monitoring activities may be conducted.

(2) Users have no expectation of privacy on GSA IT systems. All activity on GSA IT systems is subject to monitoring.

(3) GSA performs electronic monitoring of email messages transmitted out of the GSA enterprise messaging services environment for leakage of Personally Identifiable Information (PII) and/or sensitive data (e.g., Social Security Numbers, Credit Card Numbers, etc.) without required encryption as stipulated in paragraph 7.c.

(4) To ensure system reliability, the GSA enterprise messaging services system administrators/managers regularly monitor the efficient functioning of electronic messaging services, not the content of messages. These system administrators/managers review the system logs created by the various electronic messaging services to analyze service delivery problems. The logs usually contain information about each message, including sender address, receiver address, size of message, and date and time of day, but not the content of the message. These logs are retained locally for 14 days and then destroyed, if they are not being used for problem analysis. System administrators/managers only open email messages and review their content when attempting to locate a message pursuant to a request by an approved official or an OIG investigator.

(5) If system administrators/managers find indications of illegal activity or violations of Agency policy or security, they will report their findings to the appropriate ISSO/ISSM. ISSO/ISSMs must report security incidents to the OCIO SAISO in accordance with CIO-IT Procedural Guide 01-02. The SAISO will report incidents to the OIG in accordance with that Procedural Guide. All incidents involving PII must be reported to the SAISO within one hour of discovering the incident. There should be no distinction between suspected and confirmed breaches. Any incident which involves PII

and could result in identity theft must be handled in accordance with the procedures outlined in GSA Order CIO 2100.1L CHGE 1.

(6) Supervisors may request the review of the electronic messages of anyone they supervise if they have reason to suspect there has been any breach of security, violations of GSA policy, or other misconduct on the part of the associate. This may include inspection of the contents of electronic messages disclosed in the course of such monitoring or any follow up inquiry, if necessary to serve an official purpose. The supervisor will be required to explain the need to gain access to the suspected individual's message files in writing and include the purpose for seeking access to the content of the individual's messages. For contractors, the request must go through the applicable Contracting Officer. For GSA employees, the request must go to the next level of authority to whom the requesting supervisor reports and then to the Office of Human Resources Management.

(7) It is a misuse of Federal Government time and resources and a violation of this directive for anyone, including system administrators, managers, and supervisors, to peruse electronic mail or other electronic messaging services, or use Agency computer systems in any fashion to satisfy idle curiosity about the affairs of others, with no business purpose for obtaining access to the files or communications of others. Anyone engaging in "snooping" is subject to disciplinary action, up to and including removal.

c. Message Encryption. Message encryption is the use of software to render a message unreadable to everyone except the sender and its intended recipient. Users shall send external email messages including sensitive information, such as PII, procurement sensitive information, etc., with GSA-provided encryption that uses certified encryption modules in accordance with FIPS PUB 140-2, “Security requirements for Cryptographic Modules,” or using WINZIP with FIPS-197 certified Advanced Encryption Standard (AES). For more information go to https://insite.gsa.gov/employee-resources/information-technology/do-it-yourself-self-help/google-g-suite-apps/google-gmail/how-to-create-fipscompliant-zip-files

d. Disclosure.

(1) Electronic messages may be treated as Agency records for purposes of the Freedom of Information Act, 5 U.S.C. § 552 and the Privacy Act, 5 U.S.C. § 552a. As such, electronic messages or portions of them may be required to be disclosed upon a proper request. Additionally, they may be disclosed pursuant to discovery in a legal proceeding or upon request by Congress. The contents of electronic messages, properly obtained for Federal Government purposes, may be disclosed for an official purpose without the permission of the authorized user who created the message. Whenever practicable, however, the author of the message will be informed regarding further dissemination of the message.

(2) The Agency may disclose information regarding the number, sender, recipient and email addresses of electronic communications sent over the electronic messaging services as authorized by law.

8. Appropriate Use.

a. When using the GSA enterprise messaging services, users are doing so as authorized users and, as such, potential representatives of GSA and the Federal Government. At all times, users should seek to promote a positive image for GSA and the Federal Government. They should be careful about how they represent themselves, given that what they say or do could be interpreted as GSA or Federal Government opinion. Users should be aware that their conduct could reflect on the reputation of GSA, the Federal Government, and its associates.

b. All users have an obligation to learn about electronic etiquette, customs, and courtesies. Applicable procedures and guidelines should be followed when using electronic messaging communications, participating in electronic messaging discussion groups, and sending attachments.

(1) The use of non-verbal cues such as capitalization as a substitute for shouting, multiple exclamation points for excitement, and expression symbols for facial or other expressions must follow the prohibited usage section of the GSA Information Technology General IT Rules of Behavior and never convey any material that could be interpreted as being sexually explicit, offensive, abusive, discriminatory, or objectionable.

(2) The content of any customizable facial expressions or other expressions (emojis or similar) created by an organization for use by employees must be reviewed by the program office/business line's management before use.

c. All users have an obligation to be aware of computer security and privacy concerns and to guard against computer viruses. Users who load files brought in from outside sources on Federal Government computers, then send the files as email attachments, present a heightened risk in this area, unless the users first virus-scan all outgoing attachments before the email is sent. Users should always exercise caution when addressing email messages, as there are users of the Agency's services who are not Agency associates. This will help to avoid inadvertently sending a message meant for GSA associates and authorized users to outsiders. Finally, never use email for transmitting or storing classified data.

d. Users must exercise caution in conveying sensitive or non-public information. Such information should be treated with the same care as paper documents conveying the same information. Sensitive information is that which would be withheld from disclosure under Privacy Act, the Freedom of Information Act, procurement-sensitive information, proprietary information of GSA service partners and suppliers, or other information deemed sensitive by the Agency such as Controlled Unclassified Information.

e. Users must follow guidance per GSA Order CIO 2103.2 Controlled Unclassified Information (CUI) Policy for proper handling, marking, protecting, sharing, destroying, and decontrolling of CUI in accordance with 32 C.F.R. § 2002.16, as amended. For more information go to

https://insite.gsa.gov/employee-resources/information-technology/security-and-privacy/controlled-unclassified-information

f. When non-agency email addresses are used for agency business, the email must be copied/forwarded to an agency account within 20 business days per the Federal Records Act (44 U.S.C. 2911 as amended by Pub. L. 113-187).

9. Inappropriate Use.

a. Conveying of Classified Data or Information. Users shall never convey classified data or information in any messages sent over the GSA electronic messaging services.

b. Prohibited Activities. The activities include, but are not limited to:

(1) Use of offensive, abusive, discriminatory, or objectionable language or graphics in either public or private messages;

(2) Use of lewd or sexually explicit language or graphics that are inappropriate or offensive to co-workers or the public, such as the use of sexually explicit materials, or materials or remarks that ridicule others on the basis of race, creed, religion, color, sex, handicap, national origin, or sexual orientation;

(3) Using the GSA enterprise messaging services to misrepresent oneself, GSA, or the Federal Government;

(4) Using the GSA enterprise messaging services to "snoop" on or invade another person's privacy merely to satisfy idle curiosity and with no legitimate Federal Governmental purpose;

(5) Any use that reflects adversely on GSA or the Federal Government;

(6) Transmitting any material pertaining to GSA, the Federal Government, or any agency employee or official that is libelous or defamatory; and

(7) Automatically forwarding email messages from GSA email addresses to any non-Federal email account(s) or addresses.

c. Malicious Use and Denial of Service. Unlawful or malicious activities that would result in a denial of service to other users and abuse of resources are prohibited. Malicious use is designed to embarrass, harm, or otherwise cause others to suffer. Denial of service is one type of malicious use. Denial of service is any activity that interferes with official GSA or Federal Government business by overloading resources, or blocking access to any resources.

d. Abuse of Resources. Activities that result in no benefit to GSA or the Government, and cause the Agency additional expenses through increased load on networks, systems, and staff is prohibited. Examples include transmitting sexually explicit or offensive material, non-business related large attachments, chain letters, unauthorized mass mailings, or intentionally sending a virus/worms. Abuse of resources

refers to any use of Federal Government time or resources that is of no benefit to the Federal Government. Examples include but are not limited to:

(1) Joining electronic discussion groups (listservs, newsgroups, etc.) that are not Federal Government business-related and result in mailings to an authorized user at work;

(2) Use of the GSA enterprise messaging services for an authorized user's own private gain, for the endorsement of any product, service, or enterprise, or for the private gain of friends, relatives or persons with whom the authorized user is affiliated in a nongovernmental capacity, including nonprofit organizations of which the authorized user is an officer or member, and persons with whom the authorized user has, or seeks, employment or business relations; and

(3) Use of the GSA enterprise messaging services to solicit Agency authorized users for any purpose not related to official Federal Government business.

e. Inappropriate Signature Block Content. The signature block is the part of an email message that contains the sender's contact information. This information usually consists of at least the sender's name and phone number. A signature block might also include additional information, such as job title, department/organization, mailing/office address, email address, fax or cell phone numbers, business website address, business slogan, etc. A signature block is typically located at the end of an email message. Signature blocks are intended to be used as a method of providing sender contact information to message recipients. Only GSA and GSA business-related slogans may be used as part of a message signature block. In addition, use of graphics in the signature block should be limited and is restricted to GSA and GSA business-related logos, such as the GSA logo/seal.

10. Record keeping of Email Messages.

a. E-mail recordkeeping is governed by National Archives and Records Administration (NARA) directives. Authorized users are responsible for maintaining their files within assigned storage limitations and NARA records management requirements. Authorized users are advised to apply the same decision-making process to email for records maintenance and disposition that they apply to other correspondence and documentary materials

b. The GSA electronic mail system is not an authorized records storage system for GSA records management purposes. Any records created or received in the GSA electronic mail system must be moved to a records management system in accordance with 36 CFR 1236.20(b). For instance, email that contains or is deemed a record should be moved to a recordkeeping system or a well-named, well-organized electronic storage location. If a message is determined to be a record as described in the Agency's Records Disposition Schedule, users are responsible for ensuring those messages are not deleted before the expiration of the NARA-approved retention period.

c. Non-record material (transitory documents, copies, and drafts) may be retained in an email system indefinitely in accordance with 36 CFR 1236.22. Transitory refers to documents of short-term interest of 180 days or less having no documentary or evidential value. Examples of transitory material are:

(1) Routine requests for information or publications and copies of replies that require no administrative action, no directive decision, and no special compilation or research for reply. Freedom of Information requests are not considered transitory material;

(2) Quasi-official notices, including memoranda and other records, that do not serve as the basis for official actions, such as notices of holidays or charity and welfare fund appeals, bond campaigns and similar correspondence;

(3) Copies of documents issued to multiple recipients. Usually, copies of documents received by recipients of email are copies, not records, and can be destroyed when no longer needed for reference. However, if any copy is used by the recipient to transact Agency business, that copy becomes a new record that needs to be preserved in the recordkeeping system, or project or subject file to which it applies.

(4) Drafts circulated for comment. In general, draft copies are not records. However, draft documents or working papers that change or annotate the draft to propose, comment on, or evaluate high-level policies or decisions or that provide unique information that contribute to the understanding of major decisions, must be preserved as Federal records; and

(5) Extraneous copies of records used or issued to conduct or transact official business. Normally, only the originator copy is the record copy. Every project should use a single electronic storage location or recordkeeping system, when practical, for project records so that recordkeeping is clear.

11. Waivers. Requests for waivers to this order must be submitted to the GSA Chief Information Officer for review and approval.

12. Explanation of Changes. Updated broken links, and clarified language in sections 7.c. and 8.c. for CUI. Revised language and removed outdated references in section 10 pertaining to recordkeeping of email messages. Updated references in Appendix A.

13. Signature.

/S/_____
DAVID SHIVE
Chief Information Officer
Office of GSA IT

APPENDIX A: REFERENCES

1. Federal Laws & Regulations.

5 U.S.C. § 552, the Freedom of Information Act

5 U.S.C. § 552A, the Privacy Act

44 U.S.C.§ 2901 *et sec.*, the Federal Records Act

44 U.S.C § 3301, the Federal Records Disposal Act

17 U.S.C. § 101 *et sec.,* the Copyright Act of 1976

Public Law 99-474, The Computer Fraud and Abuse Act of 1986

18 U.S.C. § 798, AND 50 U.S.C. § 783(b) regarding protection of Classified Information

18 U.S.C. § 1905, Which prohibits disclosure of proprietary information and certain other confidential information

41 U.S.C. § 423(a), which prohibits unauthorized disclosure of certain procurement-sensitive information, including proprietary or source selection information

5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch, particularly subpart G which deals with misuse of position

32 C.F.R. § 2002.16, as amended, prior to disseminating Controlled Unclassified Information (CUI), authorized holders must properly label CUI.

36 C.F.R. Parts 1220, 1222, 1228 and 1234, 1236, National Archives and Records Administration regulations on management of email messages

36 CFR 1236.20(b), Any official records created in the GSA electronic mail system must be moved to a records management system

36 CFR 1236.22, Non-record material (transitory documents, copies, and drafts) may be retained in an email file indefinitely

FIPS PUB -140-2 Security Requirements for Cryptographic Modules

FIPS PUB -197 Advanced Encryption Standard (AES)

2. Agency Directives.

GSA Information Technology (IT) Security Policy, GSA Order CIO 2100.1M CIO

GSA IT Security Procedural Guide: Incident Response (IR)-CIO IT Security 01-102

Personal Use of Agency Office Equipment, GSA Order ADM 7800.11A

Email Records Management Policy, GSA Order, OAS 1828.1

CIO Controlled Unclassified Information (CUI) Policy, GSA Order 2103.2