Records Management Assessment of Electronic Mail and Calendar Information Systems

National Archives and Records Administration
September 2023

RECORDS MANAGEMENT ASSESSMENT OF ELECTRONIC MAIL AND CALENDAR INFORMATION SYSTEMS[1]

INTRODUCTION

The National Archives and Records Administration (NARA) is responsible for establishing standards and conducting oversight of the management of records in all media types within federal agencies to protect rights, assure government accountability, and preserve and make available records of enduring value.[2] In its oversight capacity, and based on authority granted by 44 United States Code (U.S.C.) 2904(c)(7) and 2906, NARA inspects electronic records at agencies to ensure compliance with federal statutes and regulations and to investigate specific issues or concerns. NARA then works with agencies to make improvements based on its findings and recommendations.

This report addresses the Peace Corps' and the U.S. Equal Employment Opportunity Commission's (EEOC) management of records maintained in their electronic mail (email) and calendar information system. This system assessment was performed to provide objective analysis, findings, and recommendations to assist the Peace Corps and EEOC as well as other federal agencies' management and those charged with governance and oversight to:

1. Improve program performance and operations;
2. Facilitate decision-making, and;
3. Contribute to public accountability.

For this system assessment, we reviewed reports, email messages, calendars, Capstone records, non-Capstone records, data, and metadata provided by both agencies' staff. The majority of the evidence was collected through interviews that were conducted virtually. We evaluated performance and compliance against the Federal Records Act, NARA's implementing regulations in 36 C.F.R. Chapter XII, Subchapter B, NARA Bulletins, NARA's Electronic Records Maturity Model, and the U.S. Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (Green Book).

This assessment report only reflects what NARA's staff saw and heard at the time of the interviews. The documentation review and interviews were conducted between September and October 2022. Any changes to their email and calendar system since the interviews will not be reflected in this assessment report.

During this system assessment we discovered that both agencies managed, accessed, retained and preserved email and calendar records simultaneously. The environment that both these systems are maintained in are synonymous. Therefore, the reporting, findings and recommendations are

[1] Information system is defined in 44 U.S.C. § 3502(8) and refers to a discrete combination of resources organized for the processing, maintenance, use, sharing, dissemination, or disposition of information.
[2] 44 U.S.C. Chapter 29; see also https://www.archives.gov/about/laws/records-management.html.

explicitly for the system environment which includes emails, calendars and other functions unless stated otherwise.

Overall, we found that both agencies are adequately managing their email and calendar records. There is room for improvement for both agencies, but the records are currently not at high risk of being lost or damaged. This report includes findings and recommendations to improve the effectiveness and efficiency of Peace Corps and EEOC email and calendar records management.

GENERAL TECHNICAL OVERVIEW

The Peace Corps and EEOC have either recently completed a cloud migration for email systems or are currently in the process of a cloud migration. As there is perhaps no more relevant and topical subject matter in email management than its relationship with cloud computing, we felt that the lessons learned from this assessment would be instructive to other agencies that have yet to move to a cloud-based email system or have recently completed such a transition. This report provides a technical analysis for each agency individually with specific findings and recommendations that could also apply to similarly sized agencies. Further technical analysis is included in Appendix B.

Both agencies use their email and calendar system as part of their regular business practices to communicate, pass documents electronically, and schedule events. The setup of the two agencies' email systems are different despite both utilizing Microsoft as their email and calendar provider. One agency manages its email in the cloud, while the other uses on-premises servers. Despite having differing configurations, both agencies rely on the Microsoft included tools for security, privacy and storage. Both agencies rely on the litigation hold function within Microsoft Outlook as a way of managing Capstone emails. Both email and calendar are integrated into the Microsoft Exchange environment. The accessibility, security, retention rules and preservation happens together and are not segregated. Ultimately, the final transfer of both sets of information to NARA comes in the form of a personal storage table (PST) file which contains both sets of objects.

PEACE CORPS MANAGEMENT OF EMAIL AND CALENDAR RECORDS

The Peace Corps is an independent agency organized into three regions and operates in over 60 countries. Its mission is to deploy volunteers to promote world peace and friendship[3]. The Peace Corps is divided into two distinct categories -- headquarters (HQ), based in Washington, DC, and overseas posts. At the time of the interviews, there were 66 active posts. The Agency Records Officer (ARO) informed us during the interview process that they will soon be moving to Microsoft Office 365 and using cloud computing for their email. However, the process was not fully planned out at the time of the interviews. This report will not analyze their future email system; rather, it will focus on their current system.

The Peace Corps manages email under General Records Schedule (GRS) 6.1 and has a NA-1005 Verification Form approved by NARA in 2018. There are currently 45 accounts subject to

[3] "About," Peace Corps, last accessed April 28, 2023, https://www.peacecorps.gov/about/.

Capstone management. All of the Capstone accounts are located at HQ. Peace Corps does not create emails for permanent retention at any post unless an email or calendar is sent from or to a Capstone official at HQ.

The Peace Corps currently uses Microsoft Exchange for email communication. The infrastructure is set up on-premises and consists of a database availability group (DAG), which gives it a High Availability (HA) and a site resilience framework built into the Microsoft Exchange Server.

EEOC'S MANAGEMENT OF EMAIL AND CALENDAR RECORDS

The Equal Employment Opportunity Commission (EEOC) is organized into 53 field offices in 15 districts nationally. Its mission is to administer and enforce civil rights laws against workplace discrimination.

EEOC has recently completed a migration from an on-premise email system (Groupwise) to Microsoft's cloud-based Office 365 (M365) email system.

EEOC migrated from Groupwise email to M365 email in 2018. Prior to that migration, email records may have been backed up to individual Compact Discs (CDs) and given to supervisors for archiving. Since the migration, all records are backed up in the Azure cloud in M365 and in an independent archive, AvePoint. AvePoint is a third-party software as a service (SaaS) product that EEOC uses to further backup its emails and SharePoint for redundancy.

Upon completion of the migration to M365, EEOC issued guidance to Capstone officials in an email notice which informed them that:

> "We have completed your GroupWise Archive migrations…. We also have configured your mailboxes, per the attached memorandum, so that you may no longer permanently delete emails. As a practical matter, you can manage your mailbox in any manner you have been or wish to, including deleting emails. However, any emails you delete will still be retained within Office 365 and will (1) be recoverable, (2) still be considered records and (3) be transmitted to NARA for permanent retention as Federal records."[4]

This email further informed Capstone officials how to locate the Groupwise archive in their new Outlook folder structure. The Groupwise to M365 was successful according to EEOC. They compared byte size from Groupwise to M365 using automated tools as a way to determine a successful migration. EEOC did admit that some files were corrupted during migration with some files restored from backups. Data corruption most likely occurred due to the age of Groupwise. Once the Groupwise emails were migrated to Microsoft Exchange, they were converted to a PST file format. There is an unknown number of possible records lost due to the lack of a policy for preserving emails under Groupwise. Maintaining emails was manual, and prior to 2014, there was

[4] Peace Corps Documentation, 170807 RE_ GroupWise Archive Migration _ Capstone Designation Updates, Email, September 2022.

no data preservation policy enacted by the agency.

There are currently 41 designated Capstone officials at the EEOC. Prior to the migration of the email system to M365, users could choose what, how and when to preserve emails for permanent retention. Since the migration to M365, EEOC began managing their emails using the Capstone approach. Their policy states that emails of a Capstone official became permanent as of the year 2017, while temporary emails would be managed for seven years starting in the year 2019. At the time of the interview, EEOC did not have an approved GRS 6.1 record schedule. The draft copy of the GRS 6.1 schedule was awaiting internal senior management approval. Despite not having an active schedule, EEOC is managing their permanent email using the Capstone approach and the first transfer to NARA of permanent email is due in 2032.

EEOC provided documentation on the metadata that will be transferred to NARA by its scheduled date. Outlook keeps all the metadata, and it is wrapped in the PST. Additionally, Outlook voicemail is saved to the PST and will be transferred to NARA. However, peer-to-peer chat is currently an internal function. EEOC utilizes Microsoft Teams for internal texting/chat. Teams text messages are retained following the in-place O365 retention schedules and are covered by litigation hold policies as implemented. We were informed that external chat is something the EEOC is looking to implement soon. Once external chat is activated, the chats of Capstone officials will be subjected to GRS 6.1 rules.

EEOC provided a variety of technical documentation associated with the management of email in M365. They show that technical policies are in place for off-boarded user email retention, as well as active user email retention. Additionally, automated scripts for disabling users are in place. PowerShell scripts and Power Automate (workflow tool) are used by the Office of Information Technology (OIT) Messaging Team to implement the assigned retention policies to user accounts. The accounts for off-boarded users are disabled on close of business of the day specified in the ServiceNow off-boarding ticket. Automated scripts convert the mailboxes to "shared" and implement the offboarding retention policy. Litigation hold supersedes all retention policies.

SIMILARITIES AND DIFFERENCES

CAPSTONE

Both agencies are currently using the General Records Schedule (GRS) 6.1 schedule to manage email and calendar records. GRS 6.1 is commonly referred to as the Capstone approach to managing email and calendar records. Peace Corps currently has an approved Capstone schedule; conversely, EEOC does not yet have an approved schedule, but they are managing their permanent email using the Capstone approach.

Both agencies have designated their highest officials as having Capstone accounts. All of the email, attachments, calendar events and most of the associated chats will be transferred to NARA as permanent records.

LITIGATION HOLD FEATURES

Both agencies use the litigation hold feature in Microsoft Exchange to keep all the email and calendar records. This allows all records to be kept and preserved regardless of the actions of the account user. Using the litigation hold feature doesn't allow for active culling of records to ensure only business critical emails are preserved permanently. The user of the account can delete and move emails around, but the changes only appear in the user view. On the Microsoft Exchange server, whether on premises or in the cloud, all records are being retained if litigation hold is active on the account. Emails can be culled once litigation hold is turned off. Depending on the agency's policy, if litigation hold is deactivated prior to transfer to NARA records may be culled but otherwise, temporary and non-record material may be transferred to NARA as a permanent record.

AGENCY SUMMARY MATRIX

	Peace Corps	EEOC
Use of Litigation Hold to Meet Capstone Requirements	Yes	Yes
Fully Cloud Based	No (On Premise, future cloud migration planned)	Yes
Approved Schedule	Yes	No
International Correspondence	Yes	No
Use of Multifactor Authentication	Yes	Yes
Mobile Device Policy	Use of Government issued or personal phones. Organizational policies applied to apps on both.	Use of Government issued or personal phones. Organizational policies applied to apps on both.
Zero Trust Rules	Yes - partially	Yes - partially
Individual File Encryption	Yes	Yes
Are Hyperlink Targets Captured And Preserved For Transmission to NARA?	No	No

FINDINGS AND RECOMMENDATIONS

Finding 1: Capstone emails are being preserved using the litigation hold feature.

A litigation hold is a feature in Microsoft Exchange that allows agencies to preserve email messages and other data related to a legal matter or investigation. When a litigation hold is enabled, the data is protected from deletion or modification, even if the user or application attempts to delete it. Both the Peace Corps and EEOC use the litigation hold feature of Microsoft Exchange for maintaining Capstone email records. Litigation hold could lead to inefficient records management because there is a possibility of having all emails kept and therefore not being managed at all. This poses several possible outcomes including:

- Business critical emails that are permanent records are intermingled with personal, non-record, and temporary emails.
- The size of the mailbox may be extremely large.
    - Moving and transferring such large records could be troublesome for NARA and the transferring agency.
- Additionally, e-discovery can become an issue due to the amount of emails being maintained.

Litigation hold does not automatically delete temporary records. Temporary records are typically deleted according to a retention policy set by the agency, which specifies how long certain types of data should be kept before being deleted. Records must be separated from non-records in accordance with 36 CFR 1222.16, and in the case of emails a culling procedure is called for.

EEOC uses litigation hold for emails while the account user is still actively at the agency. All emails are maintained in the system, despite the user having the ability to delete and move from their view. Emails that are deleted by an employee are never physically deleted from the system until the end of their retention period.

Recommendation 1: Email records should be culled prior to transfer to NARA. Culling would separate temporary email records from mission-critical permanent email records.

Finding 2: EEOC should determine if there was an Unauthorized Disposition (UD) during their email migration.

EEOC migrated their agency's email from an on-premise server-based Groupwise system to M365 cloud-based email in 2018. The migration was successful according to EEOC's Information Technology section. To confirm a successful migration, they compared byte size from Groupwise to M365 using automated tools. Although the migration was successful, EEOC acknowledged that some files were corrupted during migration. Some files were able to be restored from backups while others were permanently lost due to any one of a multitude of issues. Additionally, there were an unknown number of possible records lost due to the lack of a policy for preserving emails under Groupwise. Maintaining emails was manual, and prior to 2014, there was no data preservation policy enacted by the agency. Further internal research by EEOC may

need to be conducted to determine if an UD needs to be reported to NARA.

See 36 CFR Part 1230 for more information.

Recommendation 2: EEOC should determine if there was an unauthorized disposition on federal records that occurred during their email system migration.[5] [6] (36 CFR Part 1230)

Finding 3: Zero Trust Network Access (ZTNA) is being used to control access to systems and secure records.

One of the participating agencies is applying Zero Trust Network Access (ZTNA) rules in some areas. Some of the key methods used for ZTNA are email authentication, two-factor authentication, password management and email encryption. ZTNA is a category of technologies that provides secure remote access to applications and services based on defined access control policies. Unlike VPNs, which grant complete access to a LAN, ZTNA solutions default to deny, providing only the access to services the user has been explicitly granted[7]. Thus far, ZTNA is applied when a former employee is rejoining the agency in a different role with no need to access information from their previous role.

ZTNA reinforces the records management controls to ensure a secure and proper records management program. *Reliability, Authenticity, Integrity*, *Usability*, *Content*, *Context and Structure* are all components of quality records management controls.[8] ZTNA is a relatively new approach to access controls of electronic systems but is being implemented more across the federal government.

As a reference, agencies should refer to the "NIST Special Publication 800-207: Zero Trust Architecture" to further understand and implement their ZTNA.[9]

Recommendation 3: A policy or procedure for implementing and/or expanding usage of ZTNA to further secure access to email systems and records should be developed.

Finding 4: Encrypted emails are not unencrypted prior to long-term preservation.

Records are increasingly at risk of being lost or unreadable due to encryption. Encryption is the process of encoding data so that it can only be accessed by those who have the correct key or password. While encryption is a powerful tool for protecting sensitive data, it can also cause problems when the key or password is lost or forgotten. Without the key or password, the data is

[5] NARA's Unauthorized Disposition Reporting Requirements, https://www.archives.gov/files/records-mgmt/resources/ud-submission-instructions.pdf.
[6] Unauthorized Disposition of Federal Records, National Archives and Records Administration, last accessed March 27, 2023, https://www.archives.gov/records-mgmt/resources/unauthorizeddispositionoffederalrecords.
[7] "What Is Zero Trust Network Access (ZTNA),"Palo Alto Networks, Inc., last accessed December 7, 2022, https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust-network-access-ztna.
[8] 36 USC § 1236.10, https://www.ecfr.gov/current/title-36/chapter-XII/subchapter-B/part-1236.
[9] *NIST Special Publication 800-207: Zero Trust Architecture"* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

essentially unreadable and can no longer be accessed. During the interview with both agencies, it was discovered that individually encrypted files were not identified, managed or decrypted when they were sent to NARA.

As the federal agency responsible for preserving and providing access to records, NARA requires that all permanent records must be transferred in an unencrypted format for preservation and eventual public access. NARA has published guidance about encrypted records in Bulletin 2007-02.[10]

In this bulletin, it states that encrypting records "could impair the ability of agencies to fulfill records management responsibilities under 36 CFR 1224.1." Encryption prevents NARA from being able to validate, authenticate and preserve records.

Recommendation 4: Peace Corps and EEOC should review their policies, procedures, and capabilities to identify a way to mitigate against the loss of encrypted records. (NARA Bulletin 2007-02)[11]

Finding 5: Emails are not scheduled with a Records Control Schedule or General Records Schedule.

At the time of the data gathering and interview, EEOC did not have an approved GRS 6.1 record disposition authority, nor were their agency's emails scheduled under an agency-specific records control schedule. The records management staff have created a draft of the NA-Form 1005, Verification Form, required to use GRS 6.1. The draft copy is awaiting internal senior management approval before it is forwarded to NARA. Despite not having an active schedule for their email, they are managing their email using the Capstone approach. They are currently managing their emails as follows:

- Retention for Capstone emails starts and dates back to 2017.
- Retention for temporary emails starts and dates back to 2019.

EEOC plans to transfer their first email records to NARA in 2032. The first email records will be dated from 2017.

Recommendation 5: EEOC's draft of the GRS 6.1 Verification Form must be finalized internally and the ARO should work with their NARA Appraisal Archivist to obtain NARA approval. (36 USC § 1220.34)[12]

[10] National Archives Bulletin 2007-02, Guidance concerning the use of Enterprise Rights Management (ERM) and other encryption-related software on Federal records, https://www.archives.gov/records-mgmt/bulletins/2007/2007-02.html.
[11] National Archives Bulletin 2007-02.
[12] 36 USC § 1220.34, https://www.ecfr.gov/current/title-36/chapter-XII/subchapter-B/part-1220/subpart-B/section-1220.34.

Finding 6: EEOC does not have an Email management training program or requirement.

EEOC does not have a required training course for Capstone officials. They are using the litigation hold function as a justification for not having required training in place. Litigation hold preserves all contents of the email account without any action from the user. EEOC mentioned that they had a training course in the development stages that is intended for Capstone officials. The training course should be implemented after their email schedule is approved.

Peace Corps works with NARA to incorporate all the required components of their records management training program and tailor it to the needs of the Peace Corps. Every Capstone official gets a detailed brochure about records management, and an in-person briefing that includes information about email recordkeeping.

*Recommendation 6: EEOC must investigate developing and implementing a required email management training for employees. (*NARA Bulletin 2017-01)[13]

Finding 7: Emails continue to be permanently preserved for officials who are no longer in a Capstone role.

Peace Corps has a policy that states if an employee is acting in a Capstone position for more than 60 days, their emails become permanent for that employee from that point on, no matter if the employee reverts to a non-Capstone position in the future.

Conversely, EEOC has developed a script that allows the emails of an employee while in a Capstone role to be preserved as permanent. The script will capture just the emails set within the start date and end date of a Capstone appointment. Once an account holder is removed from the Capstone position, the emails from that point forward are again temporary and are managed as such.

According to GRS 6.1, emails of non-Capstone officials are designated as temporary, whereas those of Capstone officials are permanent. When an individual no longer occupies a Capstone position, their records are not considered permanent from that point forward, according to this standard.

Recommendation 7: Only emails of a user while in a Capstone designated position should be considered permanent. Therefore, the Peace Corps should develop a strategy to only capture emails while a user is in a Capstone designated position. (NARA Bulletin 2013-02)[14]

[13] National Archives Bulletin 2017-01, Agency Records Management Training Requirements, https://www.archives.gov/records-mgmt/bulletins/2017/2017-01-html.
[14] National Archives Bulletin 2013-02, Guidance On A New Approach To Managing Email Records, https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html.

OTHER AREAS OF NOTICE

(There are other areas of notice found during the assessment worth noting as a best practice or where there is no recommendation being made.)

Area of Notice 1: Emails transmitted outside of the agency email system are governed by agency policies.

With both the Peace Corps and EEOC we noted that there can be occurrences when emails are transmitted outside of the agency Microsoft Exchange environment. Both agencies' policies discourage the use of non-official messaging systems except in rare circumstances. For example, the EEOC uses Secure Share for communication with court systems and other entities; Whether these communications are scheduled as permanent records is not completely clear; however, there is no independent information archive outside of Microsoft Exchange for capturing any that may be considered such.

EEOC uses an Azure cloud-based service, Secure Share, for accessing sensitive data and for sending secure emails. It is not part of the M365 suite. Since Secure Share is a standalone application that is not part of the M365 suite, there is no linkage between a Capstone user's Microsoft Exchange account and the message transmitted via Secure Share EEOC mentioned that the activity in Secure Share is logged, but the log shows an action in Secure Share and does not show the content of that action.

EEOC and Peace Corps both have policies that govern emails transmitted outside of the agency's Microsoft Exchange server. Both agencies' policies state that if sending or receiving a record using a non-official electronic messaging account, they are responsible for copying or forwarding a complete copy of the email record to an official email account not later than 20 days after the original creation or transmission of the record.[15]

Area of Notice 2: Chat messages are being managed alongside and in conjunction with email.

Both Peace Corps and EEOC mentioned the use of chat messages in their assessment interviews. They both allowed chats for all users as part of their Microsoft Exchange system. At the time of the interviews, chats were only allowed for intra-agency communication. Chat messages created in Teams are captured and linked to an employee's M365 email account. Both agencies capture chats alongside their email. Both agencies apply the same retention schedule to their chats as they do emails.

EEOC is preparing to deploy Teams-based texting technologies and policy guidance that will allow business-related chats with external parties to be maintained within Teams and managed by current retention/hold policies.

In 2023, NARA updated and expanded the GRS 6.1 guidance to further include chat messaging

[15] Peace Corps Documentation, MS-892 Records Management, https://files.peacecorps.gov/documents/MS-892-Policy.pdf.

records into the Capstone approach.[16]

(FAQs about GRS 6.1, Email and Other Electronic Messages Managed under a Capstone Approach)[17]

Area of Notice 3: All metadata expected for transfer may not be possible due to several limitations.

The metadata expected for transfers of permanent email records to NARA may not always be possible to transfer due to archival limitations and system design and implementation. According to NARA Bulletin 2013-02,[18] email records must comply with 36 CFR 1236.22, Parts (1) and (3) as stated in Section 5, Part E. These parts of the CFR require that:

> (1) The names of sender and all addressee(s) and date the message was sent must be preserved for each electronic mail record in order for the context of the message to be understood. The agency may determine that other metadata is needed to meet agency business needs, e.g., receipt information.
>
> (3) If the electronic mail system identifies users by codes or nicknames or identifies addresses only by the name of a distribution list, retain the intelligent or full names on directories or distributions lists to ensure identification of the sender and addressee(s) of messages that are records.

With regards to part (1), metadata that is necessary to meet business needs could include hyperlinks to external sources. The extent to which all other agency-specific required metadata has been identified and is properly captured in Microsoft Exchange includes all expected email related items (e.g., dates, subjects, recipients, etc.,). However, there is a limitation that messages sent to groups will only capture the group name and not the members of the group on the final PST transfer to NARA. This lack of group member names is not in compliance with the CFR part (3) that requires that the names of the members of the group be identifiable. The lack of identifiability also includes lack of blind carbon copy (BCC) recipient names. For example, BCC is intended to be kept private when it is transmitted into an email inbox and thus, it cannot be seen when the email account is converted to a PST. Unless agencies have a third-party tool that can extract this data before the account is offline, more than likely metadata like BCC and expanded groups will be lost.

---

[16] National Archives Bulletin 2023-02, Expanding the Use of a Role-Based Approach (Capstone) for Electronic Messages, .https://www.archives.gov/records-mgmt/bulletins/2023/2023-02

[17] Frequently Asked Questions (FAQs) about GRS 6.1, Email and Other Electronic Messages Managed under a Capstone Approach, https://www.archives.gov/records-mgmt/grs/grs06-1-faqs.html.

[18] National Archives Bulletin 2013-02.

SELECTED EMAIL RECORDKEEPING REQUIREMENTS IN 36 C.F.R. § 1236.22(A)

Requirement to retain and manage:	**Is Peace Corps compliant?**	**Is EEOC compliant?**
Names of sender and all addressee(s)	Yes. Sender, Carbon Copy (CC:) recipient addresses, and Blind Carbon Copy (BCC:) recipient addresses are captured in the Peace Corps record archive. However, once converted to PST, enumeration of a group is not possible.	Yes. Sender, Carbon Copy (CC:) recipient addresses, and Blind Carbon Copy (BCC:) recipient addresses are captured in EEOC's record archive. However, some correspondence with the courts might take place in Secure Share.
Date message sent	Yes.	Yes.
Attachments to electronic mail messages that are an integral part of the record	Yes. Documents attached to an email are retained as embedded data. Note: Hyperlinks internal to Peace Corps are not usable when transferred to NARA. Also, there is no mechanism to capture the target of hyperlinked information from any source.	Yes. Documents attached to an email are retained as embedded data. Note: Hyperlinks internal to EEOC are not usable when transferred to NARA. Also, there is no mechanism to capture the target of hyperlinked information from any source.
Intelligent or full names of directories or distribution lists	Yes. Directories and distribution lists are captured, but it is unclear whether the membership of a group reflects current members or the membership at the time the email was sent.	Yes, all participant lists and meeting dates are saved on Microsoft Exchange.
Calendars that meet the definition of Federal records [and governed by GRS 5.1 and 6.1]	In-part. Responses to calendar invitations (e.g., accept, maybe, decline) are separately captured in Microsoft Exchange, but are not part of the calendar object. Modern collaboration suites, including M365, generally facilitate document sharing with a single, centralized, document and access controls. Because of this, "attachments," including images, are frequently not preserved if linked/contained outside the email itself.	In-part. Responses to calendar invitations (e.g., accept, maybe, decline) are separately captured in Microsoft Exchange, but are not part of the calendar object. Modern collaboration suites, including M365, generally facilitate document sharing with a single, centralized, document and access controls. Because of this, "attachments," including images, are frequently not preserved if linked/contained outside the email itself.
Draft documents that are circulated and which meet the criteria in 36 CFR 1222.10(b)	Yes.	Yes.

CONCLUSION

The management of email and calendar records is challenging, but both the Peace Corps and EEOC are making positive steps toward overcoming obstacles. The refinement of procedures and controls, and the integration of records management and information technology processes will help the agencies better manage their records. The recommendations provided to these agencies could also help other agencies of similar size that are working to improve email and calendar records management.

The recommendations in this report are made to minimize risks to federal records, and to provide assurance that trustworthy information is available to NARA when scheduled records transfers occur. They are intended to help the EEOC and Peace Corps comply with federal statutes and regulations and ensure the timeliness, accuracy and completeness of records transferred to NARA. We have provided specific guidance in terms of the CFR and GRS where applicable as the basis for our recommendations.

During the agency comment period of the assessment report writing process, both EEOC and Peace Corps informed NARA that some of the findings and recommendations stated in the report are no longer valid. Since the interview period in September and October 2022, both agencies have implemented new policies, systems and procedures for email management. The findings and recommendations reflect the state of the agency's systems and policies at the time of the initial interviews.

APPENDIX A
INSPECTION PROCESS

OBJECTIVE AND SCOPE

The objective of this system assessment was to determine how well the participating agencies complied with federal records management statutes and regulations and to assess the effectiveness of their RM policies and procedures as they relate to email and calendar records. We evaluated them against the Federal Records Act, NARA's implementing regulations in 36 C.F.R. Chapter XII, Subchapter B, NARA Bulletins and Electronic Record Maturity Model, and the U.S. Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (Green Book).

Two agencies participated in this system assessment, each with differing email systems, third-party tools, and uses for email communication. For this system assessment, NARA focused on the way these agencies managed their permanent email, how they secured their email systems and the data within and how they managed the migration from one system to another.

METHODOLOGY

The methods employed included generating pre-assessment questionnaires, document requests and reviews, and virtual interviews. The scope of the questionnaire and documents requested included what was necessary to gain an understanding of the system design and architecture, operations and maintenance and records management practices that are followed at each agency.

- Reviewed records management policies, directives, and other documentation provided by Peace Corps and EEOC's RM department;
- Interviewed program staff and IT staff virtually via teleconference; and,
- Used a detailed checklist of questions based on federal statutes and regulations, NARA Bulletins, NARA Universal Electronic Records Management (UERM) guide, and the NARA Electronic Record Maturity Model.

The goal of this system assessment was to provide RM guidance to agencies deemed small in size. Additionally, these agencies were selected due to the setup of their email system. One agency has a cloud-based system, while the other has an enterprise-based system. We determined that the stark similarities and differences would make a useful assessment for the RM community. Lastly, perhaps there is no more relevant and topical subject matter in email management than its relationship with cloud computing. We felt that the lessons learned from this assessment will be instructive to other agencies that have either yet to move to a cloud-based email system or have recently completed such a transition.

APPENDIX B
TECHNICAL BACKGROUND

TECHNICAL ANALYSIS OF THE PEACE CORPS

The Peace Corps currently uses Microsoft Exchange for email communication. The infrastructure is set up on-premises and consists of a database availability group (DAG), which gives it a High Availability (HA) and a site resilience framework built into the Microsoft Exchange Server. The Cisco Email Security Appliance (IronPort) is a virtual appliance which provides an internal barrier, edge protection, spam filtering, virus protection and encryption for their email system. Internet email that is inbound and outbound within the Microsoft Exchange environment routes through the IronPort. All outbound mail leaves from one of the three main servers at HQ and it is encrypted to and from IronPort. Post email routes through HQ, post external email goes through HQ. External email goes through HQ. All Microsoft Exchange servers are running Microsoft Exchange 2016 on physical machines dedicated to the service. All individual servers have a single instance storage in all of them with all Microsoft Exchange roles present on each server. This gives each physical server the ability to play a primary role while others are down.

On the client side, the Peace Corps uses another layer of security, System Center Endpoint Protection (SCEP). With SCEP it can identify, quarantine, and remove Windows viruses and malware. "Endpoint Protection manages antimalware policies and Windows Defender Firewall security for client computers in your Configuration Manager hierarchy."[19] SCEP is dependent on Microsoft System Center Configuration Manager to deploy the SCEP agent to clients and distribute updates. But using SCEP in addition to their other security, Peace Corps can better protect their email system by configuring anti-malware policies, configuring Windows Defender firewall settings, use Configuration Manager software updates to download the latest anti-malware definition files and use in-console monitoring.

For mobile devices, the Peace Corp provides government furnished equipment (GFE) smartphones and also allows users to bring their own devices (BYOD). Email is accessed through MS Outlook Web Access (OWA) with RSA dual authentication on their mobile devices. Outlook Anywhere or Microsoft Exchange Web Services are restricted externally due to security concerns and data at rest requirements. Peace Corps uses AirWatch by VMware Software-as-a-Service (SaaS) as the Enterprise Mobility Management platform.

Peace Corps uses Symantec Backup Exec for its local site backup solution to provide recovery of requested data limited to server and user file structure. Backup Exec permits the ability to backup/restore physical and virtual systems which protect Microsoft Exchange, Active Directory, and SQL Server. Data is backed up weekly to tape and nightly to local disk according to an established schedule. The tapes are changed by the onsite personnel on a weekly basis. There is

[19] "Endpoint Protection," Microsoft Endpoint Configuration Manager Documentation, Last Modified October 4, 2022, https://learn.microsoft.com/en-us/mem/configmgr/prot ect/deploy-use/endpoint-protection.

no granular restore option for the data backed up on tapes. The Peace Corps has to restore the entire database to recover a file from the tapes.

The Peace Corps uses a Personnel Tracking System (PTS), which is used to manage personnel records for all of its employees and contractors. It initiates all staff hires, transfers, extensions updates and terminations. Once the user is created in PTS, the Capstone users are defined in Active Directory (AD) with custom attributes. This makes it easier to apply long-term retention to the records and put them on litigation hold status within the system.

TECHNICAL ANALYSIS OF THE EEOC

EEOC's M365 is a cloud-based system in the G5 Government cloud. Their system is Federal Risk and Authorization Management Program (FedRAMP) certified since ATO in 2017. EEOC uses the built-in storage that the cloud provides. As mentioned above, EEOC uses an additional storage SaaS product, AvePoint, for redundancy. All users in EEOC have G5 licensed accounts therefore making the accounts virtually unlimited in size. There are a few G3 licenses for group email and special email accounts. MS Defender is used to control spam emails. In addition, MS Endpoint Manager is used as a way to further email from spam and other malicious attacks. Despite the size of the EEOC's email holdings (nearly 300 million items in all mailboxes), no specific procedures have yet been developed for transferring permanent email and calendar records to NARA.

EEOC uses the Department of Homeland Security's (DHS) E^3A Einstein 3 to provide an additional layer of security to emails in transit. The United States Computer Emergency Readiness Team (US-CERT) and the Cybersecurity and Infrastructure Security Agency (CISA) developed Einstein 3 as a new approach in which major internet service providers provide intrusion prevention security services for federal agencies using widely available commercial technology. Einstein 3 allows CISA to both detect cyberattacks targeting federal agency networks and actively prevent potential compromises. Additionally, serves as a platform to aggregate agency traffic so that CISA can implement new and advanced protections[20]. Every incoming and outgoing EEOC email is routed through Einstein in real time and checked for malicious material; if it passes the check, the email continues to its intended destination.

EEOC typically issues government furnished mobile devices, which are secured using Microsoft Endpoint Manager, which also enables access to the Outlook app. Multifactor authentication is turned on. Additional security measures are taken, such as requiring iOS devices to be fully updated to maintain access to email. Also, international access is only allowed if a user is placed in a special group, restricted by Endpoint. The BYOD policy will only allow mobile device access if it is set up as a managed device, unmanaged devices are not allowed access.

EEOC also uses the Data Loss Prevention (DLP) feature in M365. DLP is used for detecting Personally Identifiable Information (PII) such as Social Security Numbers (SSN). The DLP in use is built into the Microsoft 365 suite, and triggered when an email is sent outside the EEOC

[20] "EINSTEIN," Securing Federal Networks, Cybersecurity and Infrastructure Security Agency, accessed November 30, 2022, https://www.cisa.gov/einstein.

network. When sensitive information is detected in an email, that email is flagged and reviewed by a member on the Privacy Team. The review of an email is a manual process. Emails flagged by the DLP are automatically rejected if a decision is not rendered from the Privacy Team within 48 hours. Unfortunately, the DLP can only read attachments in emails that are machine readable. For example, a PDF with PII may not be detected by the DLP if the PDF is not readable (e.g., contains information in an image format rather than text).

BIOMETRIC AUTHENTICATION

One characteristic of this system assessment is that the use of multifactor authentication, and in particular biometric authentication, is increasing as both agencies employ it on their mobile devices. The importance of biometrics is that it is one tool available to provide multi factor authentication for access to records. This enhances the security posture and helps ensure the confidentiality, integrity and availability of records. There are multiple strategies for biometric identification, the most common of which are fingerprint and facial recognition. On Apple iOS devices, facial recognition (Face ID) is typically used on modern devices, whereas on Android devices, fingerprint recognition is typically used on modern devices. There is continuous debate within the IT and mobile security community on which biometric identification style is more secure. Each approach has its advantages and disadvantages. This is an on-going debate that needs to be monitored by IT departments in order to secure data on GFE and BYOD equipment.

APPENDIX C
RESOURCES USED

AvePoint SaaS and Data Management Platform, https://www.avepoint.com/

Endpoint Management at Microsoft, https://learn.microsoft.com/en-us/mem/endpoint-manager-overview

Cybersecurity and Infrastructure Agency (CISA) https://www.cisa.gov/einstein

Cybersecurity and Infrastructure Security Agency. "EINSTEIN." Securing Federal Networks. accessed November 30, 2022. https://www.cisa.gov/einstein.

Microsoft Corporation. "Endpoint Protection." Microsoft Endpoint Configuration Manager Documentation. Last Modified October 4, 2022, https://learn.microsoft.com/en-us/mem/configmgr/prot ect/deploy-use/endpoint-protection.

Microsoft Corporation. "How Windows uses the Trusted Platform Module." Windows Security. last accessed December 9, 2022. https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/how-windows-uses-the-tpm.

Microsoft Corporation. "In-Place Hold and Litigation Hold in Exchange Online." Security and Compliance for Exchange Online. June 9, 2022, https://learn.microsoft.com/en-us/exchange/security-and-compliance/in-place-and-litigation-holds

Microsoft Corporation. "Microsoft Pluton Security Processor." Windows Security. last accessed December 9, 2022. https://learn.microsoft.com/en-us/windows/security/information-protection/pluton/microsoft-pluton-security-processor.

National Institute of Standards and Technology. *NIST Special Publication 800-207: Zero Trust Architecture."* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Palo Alto Networks, Inc. "What Is Zero Trust Network Access (ZTNA)." accessed December 7, 2022, https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust-network-access-ztna.

Peace Corps, "About," https://www.peacecorps.gov/about/.

Peace Corps Documentation. 170807 RE_ GroupWise Archive Migration _ Capstone Designation Updates, Email, September 2022.

Peace Corps Documentation. MS-892 Records Management, November 9, 2020. https://files.peacecorps.gov/documents/MS-892-Policy.pdf.

Secure Share Delivery Portal, https://secure-share.com/

APPENDIX D
AUTHORITIES AND REGULATIONS

AUTHORITIES

- 44 U.S.C. Chapter 29
- 36 C.F.R. Chapter XII, Subchapter B
- 36 C.F.R. § 1220.34
- 36 CFR Part 1230
- 36 C.F.R. § 1239, Program Assistance and Inspections

OTHER GUIDANCE

- NARA Universal Electronic Records Management (UERM) Requirements - https://www.archives.gov/records-mgmt/policy/universalermrequirements
- NARA Bulletins - https://www.archives.gov/records-mgmt/bulletins
    - *Guidance Concerning The Use Of Enterprise Rights Management (ERM) and Other Encryption-Related Software On Federal Records* (NARA Bulletin 2007-02) - https://www.archives.gov/records-mgmt/bulletins/2007/2007-02.html
    - *Guidance on a New Approach to Managing Email Records* (NARA Bulletin 2013-02) - https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html
    - *Guidance For Agency Employees On The Management Of Federal Records, Including Email Accounts, And The Protection Of Federal Records From Unauthorized Removal* (NARA Bulletin 2013-03) - https://www.archives.gov/records-mgmt/bulletins/2013/2013-03.html
    - *Format Guidance for the Transfer of Permanent Electronic Records* (NARA Bulletin 2014-04) - https://www.archives.gov/records-mgmt/bulletins/2014/2014-04.html
    - *Agency Records Management Training Requirements (*NARA Bulletin 2017-01) - https://www.archives.gov/records-mgmt/bulletins/2017/2017-01-html
    - *Expanding the Use of a Role-Based Approach (Capstone) for Electronic Messages* (NARA Bulletin 2023-02) - https://www.archives.gov/records-mgmt/bulletins/2023/2023-02
- *General Records Schedule 6.1: Email Managed under a Capstone Approach* (NARA Transmittal Number 31) - https://www.archives.gov/files/records-mgmt/grs/grs06-1.pdf
- Federal Records Management, Unauthorized Disposition of Federal Records - https://www.archives.gov/records-mgmt/resources/unauthorizeddispositionoffederalrecords

- Frequently Asked Questions (FAQs) About Transferring Permanent Electronic Records to NARA - https://www.archives.gov/records-mgmt/faqs/transfer-erec
- Frequently Asked Questions (FAQs) about GRS 6.1, Email and Other Electronic Messages Managed under a Capstone Approach - https://www.archives.gov/records-mgmt/grs/grs06-1-faqs.html
- NARA *Criteria for Successfully Managing Permanent Electronic Records* - https://www.archives.gov/files/records-mgmt/2019-perm-electronic-records-success-criteria.pdf
- NARA *Unauthorized Disposition Reporting Requirements* - https://www.archives.gov/files/records-mgmt/resources/ud-submission-instructions.pdf
- U.S. Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government* - https://www.gao.gov/assets/670/665712.pdf
- Office of Management and Budget (OMB) Memorandum M-16-17 and OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* - https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

STATUTES AND REGULATIONS

36 CFR Chapter XII, Subchapter B, specifies policies for Federal agencies' records management programs relating to proper records creation and maintenance, adequate documentation, and records disposition. The regulations in this Subchapter implement the provisions of 44 U.S.C. Chapters 21, 29, 31, and 33. NARA provides additional policy and guidance to agencies at its records management website - http://www.archives.gov/records-mgmt/.

At a high level, agency heads are responsible for ensuring several things, including:

- The adequate and proper documentation of agency activities (44 U.S.C. 3101);
- A program of management to ensure effective controls over the creation, maintenance, and use of records in the conduct of their current business (44 U.S.C. 3102(1)); and
- Compliance with NARA guidance and regulations, and compliance with other sections of the Federal Records Act that give NARA authority to promulgate guidance, regulations, and records disposition authority to Federal agencies (44 U.S.C. 3102(2) and (3).